

2022-
2023

Business Email Compromise Course - Functional Specification

NAME: BEN NAGLE

STUDENT NUMBER: C00247271

SUPERVISOR: PAUL BARRY

SOUTH EAST TECHNOLOGICAL UNIVERSITY

Table of Contents

1 - Introduction	2
1.1 - Project Scope	2
1.2 - Functional Specification Document Scope	2
2 - Business Email Compromise Course Overview.....	3
Module 1 – What is Business Email Compromise.....	3
Module 2 – Identifying a Business Email Compromise Email	4
Module 3 – Prevention and Mitigation of Business Email Compromise	5
3 - Design Diagrams	6
3.1 - Login Page.....	6
3.2 - Main Page / Dashboard	6
3.3 - Sample Module Content Page	7
3.4 - Multiple Choice Question Sample	8
4 - Use Cases	9
4.1 - Actors:.....	10
4.2 - Use Case Descriptions.....	10
5 - FURPS.....	13
6 - Project Plan.....	14
References	<u>15</u>

1 - Introduction

1.1 - Project Scope

The aim of this project is to create a collection of electronic teaching materials (online course) that will be used to teach users about Business Email Compromise and increase general awareness around important security topics such as phishing and social engineering. The resulting “course” should be no more than one hour in duration, and needs to be graded (i.e., activities test how well the material is understood by the user).

1.2 - Functional Specification Document Scope

According to the University of Limerick, a functional specification is “a clear indication of the purpose, function, application and performance expected of the supplied material or service”. [1]

This document will outline the functionality of the system (a web application hosting an online course) and how actors will interact with it. A description of the course, such as intended module content and duration will be outlined. Design Diagrams will be provided to demonstrate the ‘look and feel’ that is intended for the web application and possible use cases will be detailed. The document intends to outline how this system will function once developed in a clear and understandable format.

2 - Business Email Compromise Course Overview

This online Business Email Compromise course will take approximately 1 hour to complete and will be broken into 3 modules that the participant must complete before progressing. After each module has been completed, the participant must undertake a quiz in which they will be required to achieve a grade of 60% and above to pass. A description and breakdown of each module is provided below:

Module 1 – What is Business Email Compromise

Topics:

- How internet email works (brief)
- Social Engineering and Phishing
- What is Business Email Compromise

Duration:

- **Content:** 15 minutes
- **Quiz:** 5 minutes

The first module of the course will provide the participant with a broad overview of how internet email works, which is important to develop context for content later covered in the course. BEC can involve the attacker performing social engineering to get the victim to comply with their request, it is vital that the participant of this course has some understanding of what social engineering is before covering BEC in more detail. By covering social engineering, the participant should be more aware of the tactics attackers use to trick victims.

BEC is a form of Phishing, as such the general topic of phishing is covered to give the participant an understanding of how BEC developed. Having established some background, the final topic will explain BEC in general terms which will introduce the participant to the subject. A definition of BEC will be provided along with some information around how the attacks generally work, the types of attacks and more detailed information will be provided in module 2.

Having completed the course content, a five-minute quiz made up of multiple-choice questions will test the participants knowledge on the above-described topics. The questions will ensure the participant has developed a good groundwork which will be important for the following modules.

Module 2 – Identifying a Business Email Compromise Email

Topics:

- How BEC attacks work and who can be targeted
- Spoofing and account compromise
- How to spot a BEC email
- Language used by attackers

Duration:

- **Content:** 25 minutes
- **Quiz:** 10 minutes

Module 2 begins by detailing how BEC attacks generally work and who can be targeted. Common types of BEC schemes will be identified and the targets generally associated with each, providing the participant with a general overview of the common types of attacks.

Methods used by attackers to conduct BEC schemes are explained, notably spoofing and account compromise. Content from module 1 will be recalled here, notably 'How does internet email work' and 'Social Engineering'. This will help reinforce content as well as expand upon it in relation to BEC.

Having established how the attacks work, the module will cover how to identify a BEC email. This topic is supplemented with language used by attackers, which can be a key clue when attempting to identify a potentially fraudulent email. Examples of BEC emails will be shown to the participant with a breakdown of clues that would suggest the email is not legitimate.

Following completion of the module content, a 10-minute quiz will test the user's knowledge on the topics covered. This quiz will be made up of multiple-choice style questions on the module content and examples of emails (some legitimate) for the user to correctly identify.

Module 3 – Prevention and Mitigation of Business Email Compromise

Topics:

- What to do if you are a victim of BEC/Phishing
- What to do if you suspect your account is compromised
- How to avoid your account being compromised

Duration:

- **Content:** 10 minutes
- **Final Quiz:** 10 minutes

The final section of this BEC course will provide the participants with steps to take if they believe that they have been the victim of Business Email Compromise. This will equip the user with the knowledge of how to mitigate possible BEC attacks. Additionally, a section will detail action that may be required if it's suspect that their account has been compromised. Earlier in the course, the user is made aware of how successful account compromise may be key for an attacker to perform reconnaissance on an organisation, this section will further enrich this knowledge by providing steps to mitigate account compromise.

Finally, a section is dedicated to avoiding account compromise which will also detail best security practices to abide by. The final quiz will have a duration of 10 minutes and will cover not only content covered in this module, but also recall some content from previous modules.

Having completed each module successfully, the participant will be provided with a breakdown of their results. A result of 60% or higher for each module quiz is required for the participant to have successfully completed the course, the course can be repeated multiple times to facilitate this. The course will have provided the participant with the knowledge and skills required to identify and mitigate potential BEC attacks as well as providing a greater understanding around key topics such as account compromise, spoofing and social engineering. These topics will provide the user with information which is important for cyber security in general.

3 - Design Diagrams

3.1 - Login Page

This Business Email compromise course is designed for organisations who will set up accounts for employees that will participate in the course. Having received their credentials from the organisation admin, users can login to their accounts from this page or reset their password. Regular users will be taken to the course dashboard/welcome page, while admins will be able to view organisation wide completion, results and create new accounts.

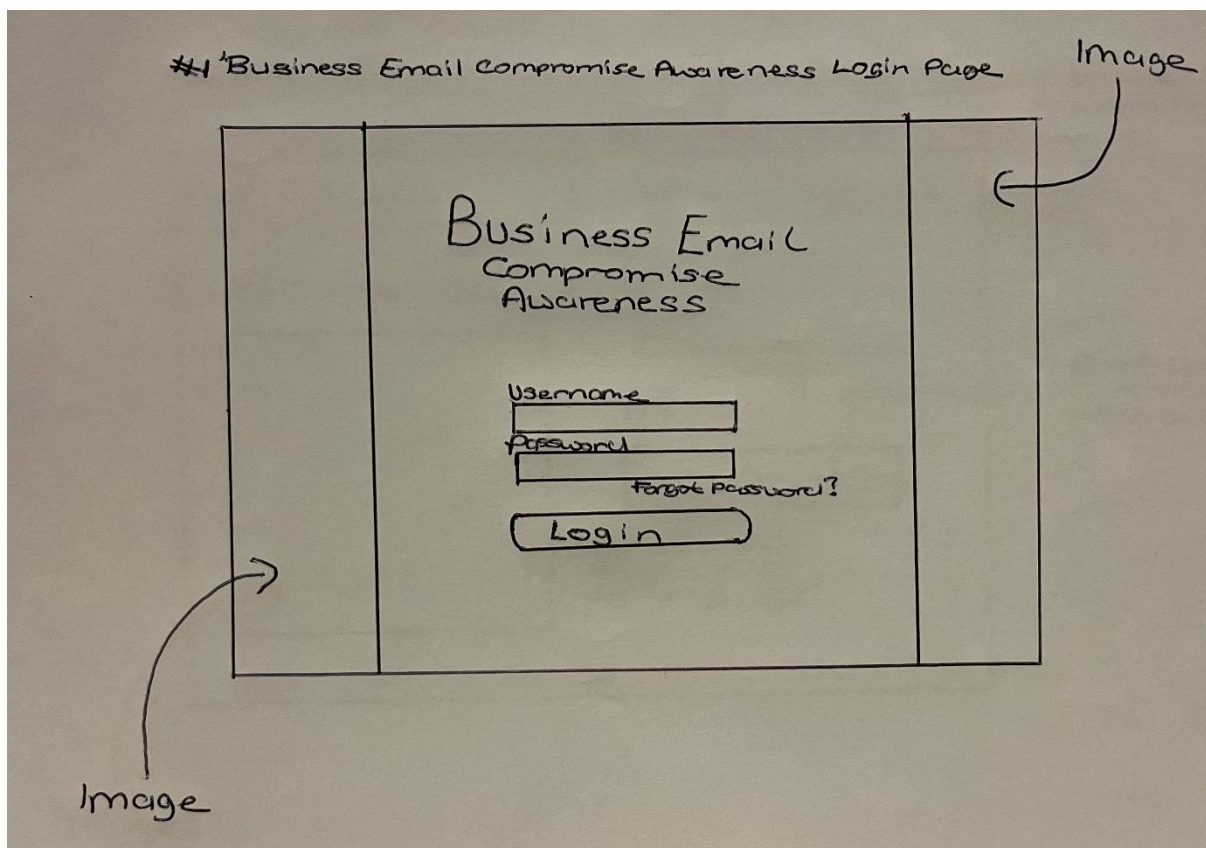


Figure 1: Login Page sketch

3.2 - Main Page / Dashboard

Having successfully authenticated as a regular user, the participant will be presented with the main page/dashboard. From here, a user may view their grades from all previously completed attempts, a 'Help' page will be available with a user guide for navigating and completing the course and the user may 'sign-out' from this page. A brief description of the

course with some key information (required pass rate, re-take policy, duration etc.) will be provided along with a break down of each modules content.

The course can be launched by interacting with the 'Begin Course' button which will take the user to the first module page.

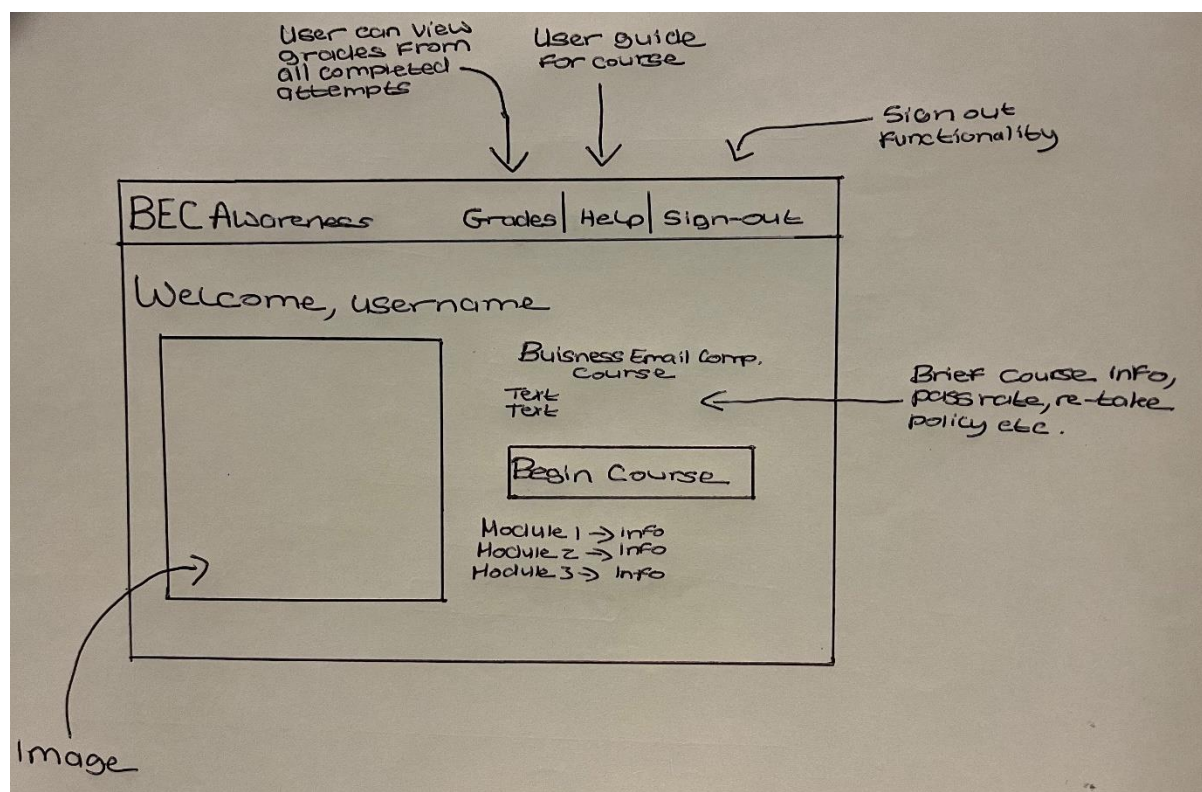


Figure 2: Main Page/Dashboard

3.3 - Sample Module Content Page

Below is a sample of a typical module content page, which the participant will interact with (primarily through reading text and viewing diagrams) during the content sections of the course. The layout of this page will depend on the material, for example sometimes diagrams or other images will be included. The participant will be able to cycle through the content pages in the module by using the 'previous' and 'next' buttons located in the bottom corners of the screen. The participant can quit the session at any time; however their progress will not be saved and they must begin the course from the beginning again.

Content will be broken up into digestible sections and will appear in bullet point form, with the use of diagrams and other images to aid visual learners.

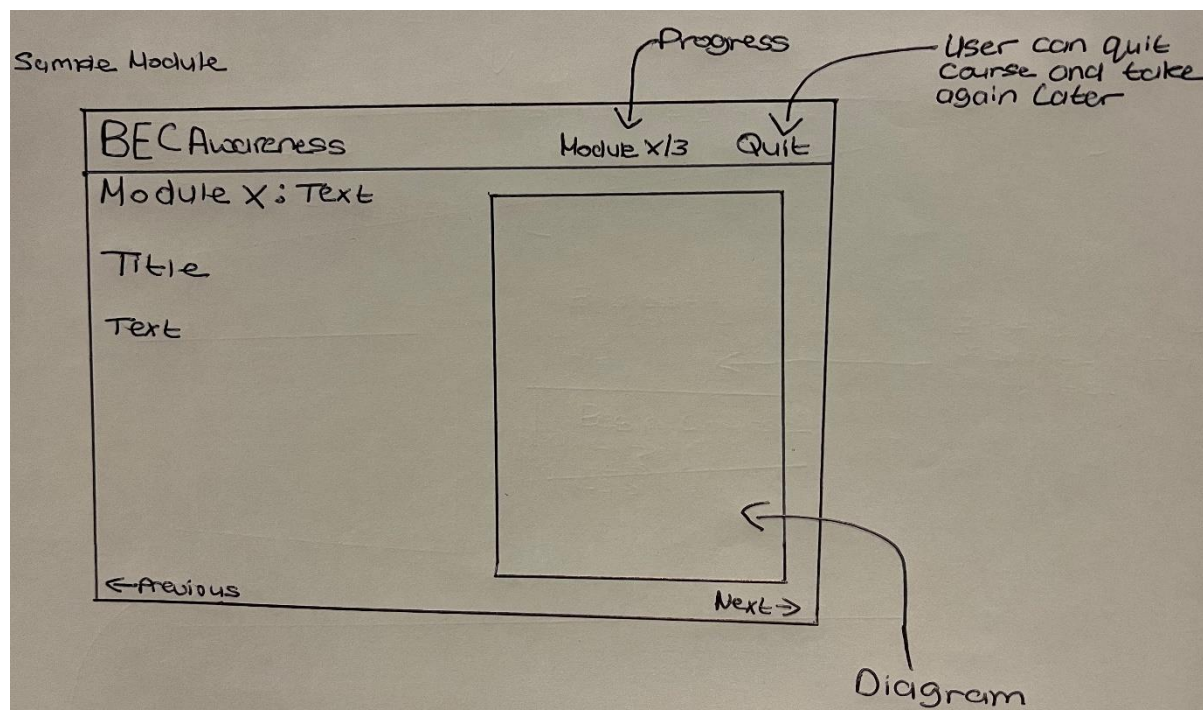


Figure 3: Sample Module Content Page

3.4 - Multiple Choice Question Sample

Below, is a sample of a multiple choice question presented to the user during an end of module quiz. Quizzes will be made up of multiple choice questions, 'fill in the blanks' and examples of BEC emails for the user to identify. The question and options will be located in the center of the page and a button to proceed to the next question will be located in the bottom left hand corner. Unlike during the module content, participants will not be able to view previously answered questions and will only be able to move forward through the quiz. Some questions will include images and diagrams, which will be placed below the question text.

Having completed the module quiz, the user will be presented with their grades. If the user achieves a pass grade ($\geq 60\%$), they will be able to proceed.

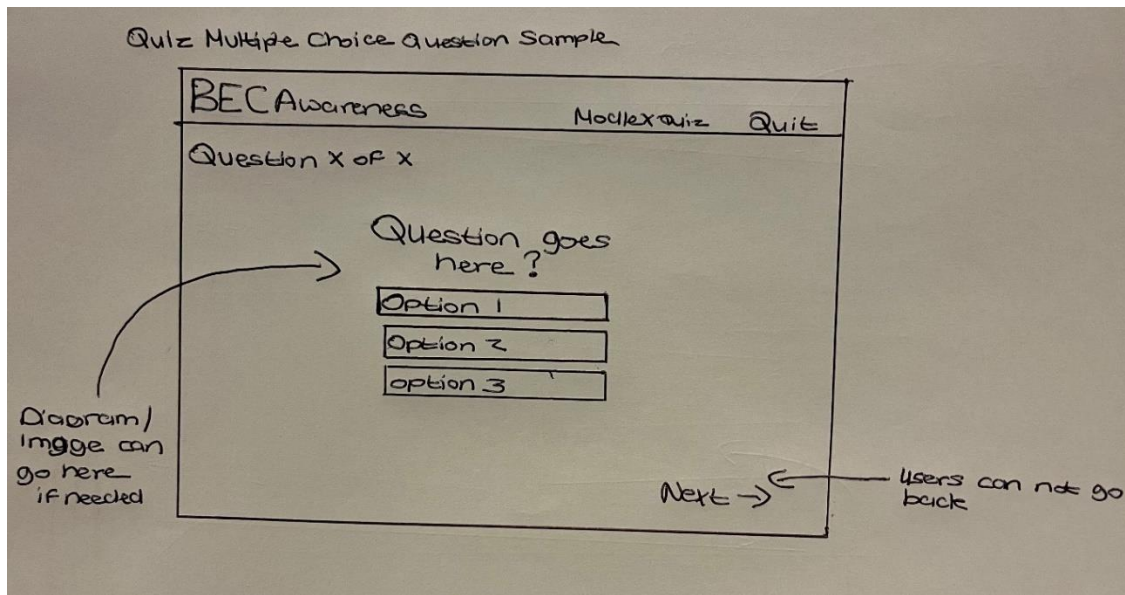


Figure 4: Multiple Choice Question Sample

4 - Use Cases

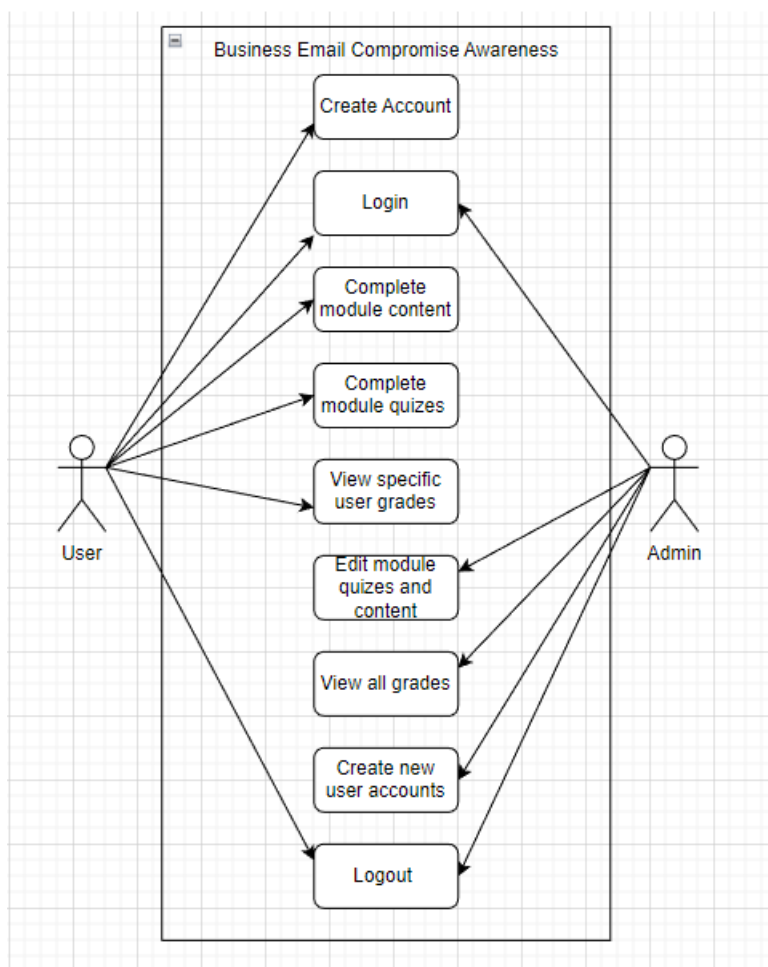


Figure 5: Use Case Diagram

The above use case diagram was designed using the online tool 'diagrams[.]net' [1], this diagram describes how users and admins will interact with the system.

4.1 - Actors:

Admins:

Admin accounts will be created for organisations who wish to enrol employees in the course. Admins will be able to authenticate through the admin portal, which will be separate to the standard user login page. Once authenticated, users with admin privilege will have several unique use cases. Single users (not part of an organisation) wishing to enrol themselves in the course will not require any access to these use cases.

Users

Regular users of the system can create their account or use credentials provided by their administrators. Users will primarily interact with the system through completing the course content and quizzes.

4.2 - Use Case Descriptions

Use Case Name	Create Account
Description	Users may create an account to enrol themselves into the course.
Primary Actor	User
Secondary Actor	None
Preconditions:	User has an email address
Postconditions:	User account is created, and system prompts user to sign in.

Use Case Name	Login
Description	Users with credentials may login to their accounts
Primary Actor	User
Secondary Actor	Admin
Preconditions:	User has an account
Postconditions:	The system displays the main page/dashboard.

Use Case Name	Complete Module Content
Description	Once the course has been launched from the main menu, users will be able to view module content as they progress through the course
Primary Actor	User
Secondary Actor	None
Preconditions:	User has signed in and launched the course
Postconditions:	System displays relevant pages and user progresses through the course.

Use Case Name	Complete Module Quizzes
Description	Having launched the course, authenticated users must complete and pass module quizzes to progress and complete the course.
Primary Actor	User
Secondary Actor	None
Preconditions:	User has signed in and launched the course
Postconditions:	System displays relevant quiz

Use Case Name	View User Specific Grades
Description	Users will be able to view their grades for each attempt of the course, users will only be able to view their own grades.
Primary Actor	User
Secondary Actor	None
Preconditions:	User has an account and is signed in
Postconditions:	System displays page with the user's grades to date.

Use Case Name	Edit module content and quizzes
Description	Admins will be able to customize the contents of the course. By default, the course will cover general BEC email examples, an admin working for a specific organisation (ex. Microsoft) may wish to tailor the examples specifically for that organisation.
Primary Actor	Admin
Secondary Actor	None
Preconditions:	Admin has signed in via Admin portal
Postconditions:	System displays page from which the admin can edit module content and quizzes.

Use Case Name	View All Grades
Description	Admins will be able to view all user grades and completion statuses.
Primary Actor	Admin
Secondary Actor	None
Preconditions:	Admin has signed in via Admin portal
Postconditions:	System displays relevant page with all user grades of interest.

Use Case Name	Create New Accounts
Description	Admins will be able to create new user accounts, including admin accounts.
Primary Actor	Admin
Secondary Actor	None
Preconditions:	Admin has signed in via Admin portal
Postconditions:	New account is created

Use Case Name	Logout
Description	Authenticated users will be able to sign out of their session.
Primary Actor	User
Secondary Actor	Admin
Preconditions:	User has signed in.
Postconditions:	System displays page informing the user they have logged out successfully. User may now close window or return to login page.

5 - FURPS

'FURPS' is an acronym for Functionality, Usability, Reliability, Performance, and Supportability created by Robert Grady [2]. It aids in categorizing the important aspects (functional and non-functional) of the system and reduces the risk of not considering them.

Functionality

The functionality of this system is explained in section () 'Design Diagrams' and section () 'Use Cases'.

Usability

This system is designed to be used by people that rely on internet email, specifically employees working in specific departments of organisations. The course will be web based and anyone with a valid email address will be able to create an account and interact with the system. To ensure usability the website will have a simplified user interface and provided help documentation will guide the user and help in navigation of the system

Reliability

The system is a website that will be available to anyone with internet access and an email address. The primary technologies being used to develop this system (HTML, CSS, and JavaScript) are supported in all web browsers as they adhere to the same standards [3].

Performance

The system should be easy to navigate and responsive to provide the user with the best experience.

Supportability

The web application will be accessible via the user's browser of choice and will not require any additional installations on the host machine as it is web based. Admins will have the ability to access the system via a dedicated portal in which changes can be made to the database, including user accounts and course content. Admins can launch the course to test any changes in content.

6 - Project Plan

Plan	Deliverable	Due Date
Research	Research Document	25/11/2022
Prepare and practice presentation	1 st Presentation to supervisors	8/12/2022
Outline/ plan functional specification	Functional Specification Document	16/12/2022
Christmas Break		
Create basic web application	Web application	16/01/2023
Create Module 1	Module 1	23/1/2023
Create first quiz (PHP/MySQL)	Module 1 Quiz	30/1/2023
Create Module 2	Module 2	6/2/2023
Create Module 3	Module 3	13/2/2023
Create Module 4	Module 4	20/2/2023
Create Module 5	Module 5	27/2/2023
Create Module 6	Module 6	2/3/2023
Implement login/logout/user creation system, user tracking		9/3/2023
Develop CSS/UI	User Interface	16/3/2023
Create Admin only pages	Admin only	21/3/2023
Test and implement any fixes	Testing	28/3/2023
Final Report	Final Report	April
Final submission	Final Submission	April

References

- [1] University of Limerick , “Guidelines on Writing Specifications,” [Online]. Available: <https://ulsites.ul.ie/finance/guidelines-writing-specifications>. [Accessed 16 December 2022].
- [2] PSPlus, “Think You've Got Your Requirement Defined? Think FURPs,” [Online]. Available: <https://www.psplus.ca/articles/think-youve-got-your-requirements-defined-think-furps/>. [Accessed 12 December 2022].
- [3] Learn How to Program , “Welcome to JavaScript and Web Browsers,” 13 December 2022. [Online]. Available: <https://www.learnhowtoprogram.com/introduction-to-programming-part-time/javascript-and-web-browsers/welcome-to-javascript-and-web-browsers#:~:text=HTML%2C%20CSS%2C%20and%20JavaScript%20are%20all%20fundamental%20web%20technologies%2C,standards%20set%20by%2> [Accessed 15 December 2022].
- [4] “diagrams.net, Online Diagram Software,” [Online]. Available: <https://app.diagrams.net/>. [Accessed 09 December 2022].