1.1 The following marks will be assigned on quality and meaningfulness for each of:

* + project brief (2.5 marks)
  + introduction of team expertise and rationale of topic choice (2.5 marks)
  + work plan (2.5 marks) ￼
  + peer review (2.5 marks)
* 1.2 Adequate structure and layout (title; authors; chapters on functions, use cases, data, interface, non-functional aspects/constraints; formatting used consistently): (5 marks)
* 1.3 Coherent description of the requirements, specifications, functions, non-functional  
  requirements or any constraints captured so far: (10 marks)
* 1.4 Coherent description of the data (10 marks)
* 1.5 Coherent description of interfaces design in correlation with functions (5 marks)
* 1.6 Reflection on legal, social, ethical, security, professional issues of the project, risk and economic aspects, environment awareness (10 marks)
* legal

**Requirements Specifications and (Interim) Prototype Implementation**

[1.1 Introduction 2](#_Toc1049568923)

[Project Brief 2](#_Toc923723170)

[Introduction of team expertise and rationale of topic choice 2](#_Toc1737184669)

[Work Plan 2](#_Toc922149402)

[Peer Review 2](#_Toc1149580282)

[1.2 Adequate structure and layout (title; authors; chapters on functions, use cases, data, interface, non-functional aspects/constraints; formatting used consistently) 2](#_Toc2009724300)

[Functions 2](#_Toc1584924765)

[Use Cases 2](#_Toc1065484459)

[Data and interface 2](#_Toc1943695198)

[Non-functional aspects/constraints 2](#_Toc963282967)

[1.3 Coherent description of the requirements, specifications, functions, non-functional requirements or any constraints captured so far 3](#_Toc448241114)

[1.4 Coherent description of the data 3](#_Toc1513278130)

[1.5 Coherent description of interfaces design in correlation with functions 3](#_Toc376809062)

[1.6 Reflection on legal, social, ethical, security, professional issues of the project, risk and economic aspects, environment awareness 3](#_Toc916465127)

# 1.1 Introduction

## Project Brief

We have chosen the ‘Workflow management system for non-crime related activity’ project, which is related to the Yorkshire and Humber Regional Organised Crime Unit (YHROCU). Within the projet

## Introduction of team expertise and rationale of topic choice

## Work Plan

## Peer Review

# 1.2 Adequate structure and layout (title; authors; ~~chapters on functions, use cases, data, interface, non-functional aspects/constraints~~; formatting used consistently)

## Functions

**Use Cases**

Unblock an account

Assign tasks

Declare task completion

View task

Export task’s data

Block an account after three unsuccessful attempts

Log in and log out

Sign up

Change due date

Search due date

Search for tasks

Manage permission to view a task

Delete tasks

## Data and interface

## Functional

**Login page:** Every user (admin or general users) would be able to log into their account with their staff number and a password. Once the information is validated, the access to their respective accounts would be granted, otherwise, access would not be granted, and the login info will have to be retyped. Each user has 3 attempts to connect, once these attempts are exhausted the account will be blocked and will have to be unlocked by an admin member.

**Sign up:** Every new user will have the ability to create they own account using their last and first name, their team and their staff number.

**Create task:** This page is used so users could create or add new tasks, but only the admin would be able to update the status and delete the task.

**View Task:** This page is created so every user could see all the tasks that are either accomplished either to do

## Non-functional aspects/constraints

**System Performance:** The system must respond swiftly to user actions like logging in or creating tasks, ensuring a seamless experience. It should effortlessly manage 1000 concurrent users without noticeable slowdowns.

**Security Measures:** User passwords must be securely hashed and stored to safeguard against unauthorized access. Data transmissions must be encrypted with HTTPS, preventing any interception of sensitive information. Login pages should have defences against brute force attacks, like temporarily locking accounts after 3 unsuccessful attempts. Admin accounts should have additional security layers, such as two-factor authentication, for added protection.

**Scalability Plans:** The system's design should facilitate easy scaling to accommodate more users and tasks. The database architecture should allow for seamless scaling by adding resources or switching to larger database systems as needed.

**Reliability Assurances:** A robust backup and recovery strategy should be in place to prevent data loss. Regular system backups must be performed to ensure data integrity. Monitoring tools should promptly detect and handle system failures or crashes.

**User-Friendly Interface:** The user interface should be intuitive and easy to navigate for all users. Clear error messages should guide users when they make mistakes, such as entering incorrect login credentials. Implement accessibility features to cater to users with disabilities.

**Compatibility Considerations:** The system should work seamlessly across major web browsers like Chrome, Firefox, Safari, and Edge. It should also be responsive and adapt well to various devices including desktops, tablets, and smartphones.

**Maintainability Focus:** Code documentation and organization should facilitate easy maintenance by future developers. Deploying updates and patches should be smooth without causing system downtime. Utilize proper version control to track changes and revert if needed.

**Legal and Compliance Guidelines:** Compliance with data protection laws such as GDPR should be ensured. Clearly visible privacy policies must be accessible to users. User data should only be utilized for its intended purposes and not shared with third parties without explicit consent.

# 1.3 Coherent description of the requirements, specifications, functions, non-functional requirements or any constraints captured so far

# 1.4 Coherent description of the data

3.Data Description

Data handled by admin are as follows:

· Tasks: with fields identifying what the task is.

· Tasks\_staff: what tasks are assigned to each staff member.

· Staff: Details of each staff member and their log in details.

**Tasks:**

Task ID – Unique identifier for the task – Going to increment each time.

Task name – Max characters 8 – Suggests what the task is for.

Task Description – Max characters 250 – Goes into more detail about what specifically needs to be done for the task to be complete.

Due date – dd/mm/yyyy the date of the task being due.

Assignee – Max digits (6) as this will be linked to the staff number – Person the task is assigned to.

Requester – Max digits (6) as this will be linked to the staff number – Person that created and assigned the task.

**Tasks\_staff:**

Task ID – Max digits(250) – Unique identifier for the task – Going to increment each time.

Assignee – Max digits (6) as this will be linked to the staff number – Person the task is assigned to.

Requester – Max digits (6) as this will be linked to the staff number – Person that created and assigned the task.

**Staff:**

First name – Max character (50) – First name of staff member.

Last name – Max character (50) – Last name of staff member.

Team – Max character (50) – The team the staff member is a part of within the organisation.

Role – Max character (20) – The role of the customer could be Admin or Staff.

Email – Max character (100) – The staff members work email that they have been assigned.

Password – Max character (15) – The password the staff member created to log in.

Staff Number – Max digits (6) – Unique identifier for the task.

# 1.5 Coherent description of interfaces design in correlation with functions

# 1.6 Reflection on legal, social, ethical, security, professional issues of the project, risk and economic aspects, environment awareness

Legal, social, ethical and professional issues related to the project involves considerations such as data privacy intellectual property and adherence to legal regulations. Ensuring compliance with laws like GDPR or other data protection regulations is crucial. Ethical considerations may include responsible AI use, avoiding bias, and maintaining transparency.

Security aspects should encompass the use of encrypted data to protect sensitive information during transmission and storage. Implementing secure access controls ensures that only authorized personnel can access data, minimizing the risk of unauthorized access.

In the legal aspect, there is the uncertainty of whether things would degenerate, to whom the company would turn, to the students behind the project? Or to themselves for trusting them too much? NDA documents were signed, which led this situation into more of a business and professional area. By signing said NDA the company has agreed to not disclose any personal information, also we both signed a client requirement document, which outlines the outcome of the project by signing this both parts have agreed to not disclose any confidential information. These students have not worked in the best conditions to create such a big project for such a large company. That is where social and ethical come in. Considering that the project has been done at a university where any material is open to any student, there could be a possibility of "data breach". This could be an issue because confidential information about young people could be leaked and therefore used against them or in the wrong manner. This issue takes on bigger proportions, in a way of getting guardians and external members involved and causing issues.

Risk Assessment and Mitigation:

1. Data Breach: Risk - Unauthorized access to sensitive data. Mitigation - Implement robust encryption, regular security audits, and intrusion detection systems.

2. legal compliance: Non-compliance with data protection laws. Migration – Stay informed about relevant regulations, implement privacy by design and conduct legal reviews.

3. ethical concerns: Risk - Unintended bias in algorithms or unethical use of data. Mitigation - Regularly review and audit algorithms, prioritize fairness, and establish ethical guidelines for system use.

4.system downtime:

5. Mitigating Intellectual Property Infringement Risk: Potential risk involves unintentional infringement on intellectual property rights. To address this, conduct thorough IP searches, secure necessary permissions, and document the development process meticulously to prevent legal complications.

6. data access control:  Unauthorized access to sensitive data. Mitigation - Enforce strict access controls, limiting access based on job roles, and conduct regular audits to ensure compliance.

7.communication security: Risk interception of sensitive data during transmission. Migration use secure protocols (eg , HTTPS), implement vpns and employ encryption for data transmission

8.Communication security:  Risk - Interception of sensitive data during transmission. Mitigation - Use secure communication protocols (e.g., HTTPS), implement VPNs, and employ encryption for data in transit.

This comprehensive approach to legal, social, ethical, professional issues, and risk mitigation ensures a robust and responsible project implementation. Regular updates and adherence to evolving standards are essential for maintaining the system's integrity and security over time.

B. Interim Prototype (35 marks)  
2.1 Significant functionality implemented – either front-end or back-end, or a combination of  
both; fully functional (30 marks)  
2.2 Code well-structured, with comments, OO where is the case; clear separation back-end  
and front-end (5 marks)  
C. Team Activity: NDAs, and meeting minutes (15 marks)  
3.1 Adequate structure and style of the minutes (as presented in lectures) including task  
allocation and systematic meeting notes: (12.5 marks)  
3.2. NDA (2.5 marks)

UML DIAGRAMS

A diagram of a network

Description automatically generated