Risk Assessment

The project uses geographical data to show asset locations on a map for the City of Bradford Metropolitan District Council. Potential hazards that are related to creating a web-based asset management interface for the City of Bradford Metropolitan Council are identified in this risk assessment. By addressing these risks, we can ensure that responsible and secure features are implemented into the system.

Key Words and definitions:

Key Word	Definition
Data Privacy and protection	Refers to the protection of private and sensitive data stored inside the system. It ensures that the data follows the protection laws, i.e. UK GDPR and Data Protection Act 2018, to prevent any misuse or breach of user data.
Data Security Measures	Technical and procedural measures that are put in place to prevent against illegal access and cyberthreats.
Liability and Data Accuracy	Obligation to keep accurate and current data in the system.
Accessibility	Ensures that everyone, including people with impairments can access the system.
Transparency and Fairness	The system must ensure fair treatment of all assets without any unintentional prejudices. Users should also be aware of how their data is being used and stored.
User adoption and engagement	Refers to the system's usability and the ability to retain and engage the users.
Data Ownership	Specifies who oversees and has the rights to the system's data. Users should be in control of their own data.
Fairness in Asset Categorisation	Ensures that asset classification procedures are impartial and free from any bias.
Quality Assurance	Includes the necessary procedures and tests to ensure that the system operates accurately with no errors.
System Downtime and Dependency	Refers to the risk of system failures or interruptions.
Cybersecurity	Safeguards the system from any hacking attempts or breaches.

Risks Table:

Legal Issues	Social Issues	Ethical Issues	Professional Issues
Data Privacy and Protection	Accessibility	Data Ownership	System Downtime and Dependency
Data security Measures	Transparency and Fairness	Fairness in Asset categorisation	Cybersecurity
Liability and Data Accuracy	User adoption and engagement	Quality Assurance	User Authentication

Legal Issues:

Data Privacy and Protection:
The system will keep and process sensitive and personal data. If the data is handled unlawfully, the UK Data Protection Act 2018 would be violated. This would result in penalties and loss of trust. To avoid breach of personal data, ensure to anonymise sensitive data where possible. Encrypt sensitive data and provide clear consent procedures on how a user's data is being used.

Data security measure:
Strong security measures, such as frequent backups and access limits, must be implemented to stop unauthorised access to user data. Ensuring adherence to data protection laws and regulations is crucial. Only authorised users can access the data due to access controls. Frequent backups decrease the chance of data loss from cyberattacks or system breakdowns.

Liability and Data Accuracy:
When developing the web interface, data accuracy and liability are important to consider. Inaccurate data on the map may cause users to make poor decisions, misuse the system, and compromise reliability. For example, displaying an asset's location incorrectly could ultimately provide the user with inaccurate information and result in inefficiencies or even community safety risks. If the data is used for important decisions, you may be liable for mistakes. Therefore, the data should be updated regularly, verified and cross-checked for accuracy before displaying it on the web interface.

Social Issues:

Accessibility:
Considering any physical limitations, the program should be made accessible to all users. To accomplish this, the application needs to adhere to accessibility standards and guidelines like WCAG (Web Content Accessibility Norms). To ensure that all users, regardless of ability, have an inclusive experience, features like keyboard navigation, screen reader compatibility and alternate text for images. The system should also accommodate assistive technologies like speech recognition software. For the user interface to be usable on a variety of devices, it must also be responsive to mobile devices.

Transparency and Fairness:
Fairness and transparency are important for gaining the user's trust. Users must be properly informed about how the system collects, uses, and stores their personal data and they must provide their consent. To prevent any prejudice, users should also be informed about the classification and representation of the assets and associated data. Users should have access to their data and should be able to adjust their information. The platform should respect their right to control their data.

User Adoption and Engagement:
The system's success depends on the user involvement and how easy it is to adopt the web interface. If it is difficult to use many consumers could hesitate to use it. The system needs to be simple to use and clear to encourage adoption. This would increase engagement, especially if it delivers relevant features and offers useful directions. Maintaining user engagement can also be achieved by offering continuing support, gathering user input and issuing frequent updates in response to this input.

Ethical Issues:

Data Ownership:
As mentioned before, users should have control over their own data and they should be informed about how it is being used, stored and shared inside the system. Prior consent should be sought before collecting this data, which is typically done through a popup. By their ownership rights, people or organisations must be able to view, update or remove their data without any interference. To avoid misuse, the system should include explicit data ownership policies and procedures that outline how data will be shared and protected.

Fairness in Asset Categorisation:
When creating the system, assets must be categorised honestly to prevent any unfair disadvantage or misinterpretation of any organisation. It ensures that every asset is handled properly. To avoid any unintentional discrimination in the system, each algorithm must undergo routine audits. Users must also have the confidence that all categories are well-supported and justified and that no group is favoured over another. Fair categorisation builds trust with the users.

Quality Assurance:
Since inaccurate data can result in poor decision-making, the data presented must be accurate and current. Before the system is used by the user, possible faults in its functioning, design and data can be found and fixed. This can be done by carrying out routine audits, checking for errors and confirming that every feature functions as planned. The system must be tested under real-world circumstances to fulfil the needs of a wide range of users. Furthermore, to increase the system's dependability, you should make sure that any updates do not unintentionally harm the quality of the interface.

Professional Issues:

System Downtime and Dependency:
This describes a faulty system due to server failures or technological difficulties. System dependency and downtime can cause serious problems since extended outages can result in service interruptions and monetary losses. Implementing a strong infrastructure and monitoring tools is necessary to mitigate these risks and guarantee system reliability. Reducing the impact of dependency can be achieved by providing backup solutions during outages.

Cybersecurity:
Cybersecurity for the web interface guarantees confidentiality and integrity of data held in the system. Maintaining strong cybersecurity standards, is essential to guard against breaches, hacking attempts as the web interface will store sensitive data. Inadequate cybersecurity safeguards may allow unauthorised access to a user's personal information, which may lead to legal problems. A key component of cybersecurity is multi-factor authentication, firewalls, encryption and regular security assessments. Reducing the vulnerabilities requires keeping the system updated with recent security updates.

User Authentication:
Role-based access control (RBAC) and multi-factor authentication are two effective user authentication techniques that should be used to assist in preventing unauthorised access to the system and protect sensitive data from cyber-attack. Strong authentication and data security procedures are put in place to safeguard user information, lower the possibility of breaches and uphold the system's credibility. To identify and address any possible security risks, administrators should be able to record user activity.