Untitled page

Risk and Mitigations

Along with meeting legal and regulatory requirements, the proposed digital solution is also shaped by professional standards, such as the **BCS Code of Conduct**. This code highlights the importance of professional responsibility and putting users' interests first. For instance, following the BCS Code of Conduct guides ethical choices when handling personal data, especially when users include children or other vulnerable people. It also supports transparency, reliability, and accountability throughout the solution's lifecycle. By adhering to recognised professional standards, the solution will be both legally compliant and ethically trustworthy to users and stakeholders.

Key Performance Indicators (KPIs)

95% successful booking completion rate
Measured using analytics tools (e.g., Google Analytics funnels) to track how many users start and successfully complete a booking.

Error rate below 5% across all user tasks
Measured using server-side error logs and application monitoring tools to record validation, system, and runtime errors.

Average page load time under 3 seconds
Measured using performance monitoring tools and browser/server response-time reports.

System uptime at or above 99%
Measured using server monitoring services that track availability and downtime over time.

90% satisfaction rating or higher in user surveys
Measured using post-booking or post-visit user feedback surveys and questionnaires.

Booking processing time below 2 seconds
Measured using backend processing logs that record the time taken to validate, process, and confirm bookings.

Risk Mitigations and Implementation

- **Encryption, secure authentication, hashed passwords**
  Sensitive user data will be protected by encrypting data in transit using HTTPS and storing passwords as hashed values rather than plain text. Secure authentication mechanisms such as session management and timeouts will be used to prevent unauthorised access. This ensures that even if data is intercepted or accessed unlawfully, it cannot be easily exploited.
- **Load balancing, failover systems, monitoring tools**
  To reduce the impact of server downtime, the system will be hosted on an infrastructure that supports load balancing, distributing traffic across multiple servers. Failover systems ensure that if one server becomes unavailable, another can take over automatically. Monitoring tools will be used to detect outages early, enabling issues to be resolved quickly.
- **Server-side validation and locking mechanisms**
  All critical validation will be handled on the server to prevent users from bypassing checks. Temporary locking mechanisms will be applied during the booking process to prevent multiple users from reserving the same ticket or room simultaneously. If a booking is not completed, the lock is released, ensuring availability remains accurate.
- **Retry logic, user alerts, API monitoring**
  Payment failures will be handled by implementing retry logic where appropriate and providing clear user alerts when a transaction fails. API monitoring will detect issues with third-party payment services, enabling administrators to respond quickly and minimise disruption to users.
- **Access control and privacy audits**
  Role-based access control will be implemented to ensure that only authorised users, such as administrators, can access sensitive system features. Regular privacy audits will be carried out to review how personal data is collected, stored, and accessed, ensuring ongoing compliance with data protection regulations.

- **Backups, restore points, and redundancy**
  Regular automated backups will be created to protect against data loss. Restore points allow the system to be recovered quickly in the event of failure, while redundancy ensures that critical data is stored in multiple locations, reducing the risk of permanent loss.
- **Strong validation**
  Strong input validation rules will be applied to all user inputs to prevent incorrect or malicious data from being processed. This includes checking formats, ranges, and required fields, reducing user error, and improving overall system reliability.
- **WCAG compliance and assistive technology testing**
  Accessibility risks will be mitigated by designing the system in line with WCAG guidelines, including clear contrast, keyboard navigation, and screen reader compatibility. Assistive technology testing will be used to confirm that the system is usable by people with disabilities, ensuring inclusive access for all users.

Regulatory & Legal Compliance (Applied)

- **UK GDPR**
  GDPR requirements will be met by minimising the personal data collected to only what is necessary for account creation and bookings. Data will be encrypted in transit and securely stored with access restricted to authorised roles only. Transparency is achieved through clear privacy notices and user consent during registration.
  Applied in the system: user registration, account management, booking records, admin access controls, and data storage processes.

- **WCAG 2.1 AA**
  Accessibility standards will be met by designing the interface using semantic HTML, providing alternative text for images, ensuring full keyboard navigation, and using readable colour contrast. These features allow users with visual, motor, or cognitive impairments to access the system effectively.
  Applied in the system: frontend user interface, navigation menus, forms, content pages, and testing with assistive technologies.

- **Copyright and Licensing**
  Copyright compliance will be ensured by using only licensed or original digital assets, including images, icons, and third-party libraries. All external resources will be properly credited or documented to avoid intellectual property violations.
  Applied in the system: website content, media assets, documentation, and third-party integrations used during development.

- **PCI-DSS**
  Secure payment processing standards will be met by using trusted third-party payment gateways rather than storing card details within the system. Payment data is handled only by the gateway, reducing security risk and ensuring compliance.
  Applied in the system: payment processing stage of the booking workflow and communication between the backend and the payment gateway.