* **Functionality : Features to be tested**
* User Authentication (login/logout)
* Data Input and Validation
* API Request Limit
* Error Handling

**Risk Identified:**

* API request limit may cause impact application performance.
* Delays in Environment Setup

**Mitigation Planned:**

* Implement rate limiting mechanism to handle API calls efficiently.
* Use backup environments or cloud-based infrastructure.

**Test Strategy:**

* Test all user actions, workflows, and edge cases.
* Verify API requests for success, failure, and error scenarios.

**Automation Plan:**

* Automation will be used for regression testing to ensure Functionalities are not affected by new code changes.

**Test Techniques**:

* Black Box Testing
* Boundary Value Analysis

**Tools**:

* Test Case Management: **JIRA**
* API Testing: **Postman**

**Deliverables:**

* Test cases for functionality.
* Test execution reports.
* **Performance : Features to be tested**
* System Response Time
* Load Handling (Concurrent Users/ Requests)
* Scalability Testing

**Risk Identified:**

* Incomplete Requirements
* High Concurrent user load may cause performance degradation

**Mitigation Planned:**

* Conduct requirement reviews with stakeholders early
* Conduct load testing to identify performance bottlenecks and optimize application resources

**Test Strategy:**

* Measure response times and system resource usage
* Simulate concurrent users to test load and scalability

**Automation Plan:**

* Automated Performance Testing tools will be used to simulate concurrent user loads.

**Test Techniques**:

* Load Testing
* Stress Testing
* Scalability Testing

**Tools**:

* Load Testing: **JMeter**

**Deliverables:**

* Test cases for Performance Testing.
* Performance Testing reports with Response Time metrics.
* **Security: Features to be tested**
* Authentication and Authorization
* Data Encryption
* Vulnerability Scanning
* Session Management

**Risk Identified:**

* High Defects Count in Security Tests
* Insufficient Authentication measures may lead to Unauthorized access

**Mitigation Planned:**

* Prioritize fixes and retest critical vulnerabilities
* Implement Secure Authentication mechanisms and encryption for sensitive data

**Test Strategy:**

* Verify secure authentication and authorization mechanisms
* Perform penetration testing to simulate real-world attacks
* Test for common vulnerabilities like SQL Injection, Cross-Site Scripting (XSS)

**Automation Plan:**

* Automated Security testing tools will be used for vulnerability scanning and penetration testing

**Test Techniques**:

* Vulnerability Scanning
* Penetration Testing

**Tools**:

* Penetration Testing: **Burp Suite**
* Vulnerability Scanning: **OWASP ZAP, Nessus**

**Deliverables:**

* Test cases for Security Testing.
* Security testing reports.