F21\_9514 ECP\_BVA\_R.A For Home module

# Equivalence Partitioning (ECP):

# Username Field:

* + ECP: Divide usernames into valid and invalid partitions.
  + Tests: Test with a valid username, an invalid username, and an empty username.

# Password Field:

* + ECP: Partition passwords into valid and invalid sets.
  + Tests: Test with a valid password, an invalid password, and an empty password.

# Search Functionality:

* + ECP: Group search queries into valid and invalid categories.
  + Tests: Test with a valid search query, an invalid search query, and an empty search query.

# User Role Selection:

* + ECP: Divide user roles into valid and invalid categories.
  + Tests: Test with a valid role, an invalid role, and no role selected.

# Date Selection:

* + ECP: Partition date inputs into valid and invalid ranges.
  + Tests: Test with a valid date, an invalid date, and an out-of-range date.

# Boundary Value Analysis (BVA):

# Numeric Input Field:

* + BVA: Test the numeric input field at its boundaries.
  + Tests: Test with the minimum valid value, just below the minimum, maximum valid value, and just above the maximum.

# Dropdown Selection:

* + BVA: Test the dropdown menu with values at the lower and upper bounds.
  + Tests: Select the first and last options in the dropdown list.

# Character Limit in Text Fields:

* + BVA: Test text input fields with character limits at their boundaries.
  + Tests: Enter text with the minimum allowed characters, just below the limit, exactly at the limit, just above the limit, and with the maximum allowed characters.

# File Upload Size:

* + BVA: Test file uploads with different file sizes at boundaries.
  + Tests: Upload a file with the minimum allowed size, just below the limit, exactly at the limit, just above the limit, and with the maximum allowed size.

# Session Timeout:

* + BVA: Test session timeout values.
  + Tests: Set the session timeout to the minimum allowed value, just below the limit, exactly at the limit, just above the limit, and with the maximum allowed value.

# Risk analysis:

# Security Risks:

* + **Scenario:** Attempt to access the "Home" module without proper authentication.
  + **Risk:** Unauthorized access could lead to security breaches.
  + **Mitigation:** Implement robust authentication mechanisms and conduct penetration testing.

# Data Integrity Risks:

* + **Scenario:** Intentionally provide invalid data during user input.
  + **Risk:** Invalid data may compromise data integrity.
  + **Mitigation:** Implement input validation checks and ensure proper error handling.

# Performance Risks:

* + **Scenario:** Simulate a high volume of concurrent users accessing the "Home" module.
  + **Risk:** Performance degradation under heavy load.
  + **Mitigation:** Conduct performance testing to identify and address scalability issues.

# Compatibility Risks:

* + **Scenario:** Test the "Home" module on different browsers and devices.
  + **Risk:** Incompatibility issues on specific browsers or devices.
  + **Mitigation:** Ensure cross-browser compatibility through testing and responsive design.

# Integration Risks:

* + **Scenario:** Integrate the "Home" module with external systems or APIs.
  + **Risk:** Integration failures leading to data inconsistencies.
  + **Mitigation:** Thoroughly test integrations and ensure proper error handling.
  + Usability Risks**:**
  + **Scenario:** Evaluate the usability of the "Home" module for users with varying levels of technical expertise.
  + **Risk:** Poor usability leading to user dissatisfaction.
  + **Mitigation:** Conduct usability testing and gather user feedback for improvements.