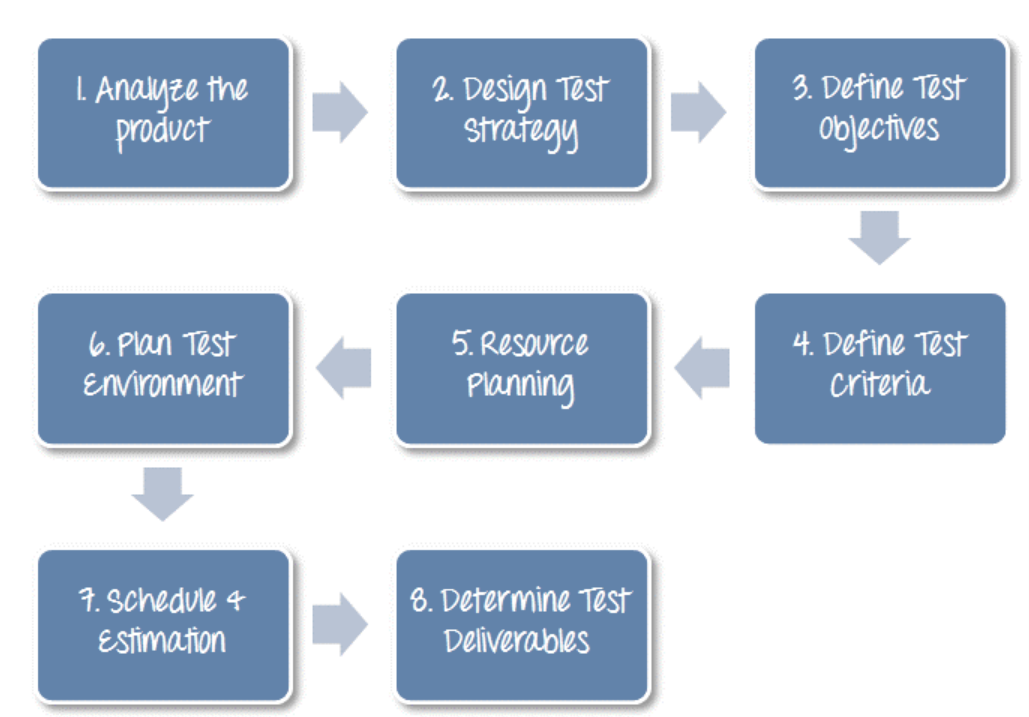
Test Plan

**Test Objective :**

**Objective** of the **testing** is finding as many software defects as possible; ensure that the software under **test** is bug free before release.

**Overview of Test Plan:**



**Product Overview :**

TQQA application works with 2 types of users i.e Active users and Super users.

Super user capabilities:

* Can create new active user with super user capabilities
* Can modify and manage any user details i.e use rid ,email and password

Active user capabilities

* Can manage details like i.e profile, edit profile and change password

Constraints:

* super user can create only 100 users through UI currently .
* Super user not able to deactivate active user through UI
* Super User can not delete any active user

**Testing Scope :**

Areas of product to be tested

1.FrontEnd testing

2.Backend testing

a)Business layer testing [API testing]

b)Database layer testing

**Types of Testing :**

**FrontEnd testing types:**

Unit Testing

### Acceptance Testing

### Visual Regression Testing

### Performance Testing

### End-to-End Testing

### Integration Testing

### Cross-Browser Compatibility Testing

**API testing types:**

Unit Testing

### Integration Testing

### Performance Testing

### End-to-End Testing

**Database testing types:**

Data Mapping Testing

Isolation Testing

Durability Testing

Data Integrity

**Automation Tools for covering all types of testing :**

Unit testing & Integration testing :pytest

FrontEnd testing :Python Framework/ Javascript Cypress

API Testing :Pytest +Requests package combination

Database testing :Pytest

E2E testing :Python Robot framework /Cypress

**High risk Areas of Application**

**Must to be covered Security areas:**

**Login Functionality:**

1. Verify that there is a limit on the total number of unsuccessful login attempts. So that a user cannot use a brute-force mechanism to try all possible combinations of username-password.
2. Verify that in case of incorrect credentials, a message like “incorrect username or password” should get displayed instead of an exact message pointing to the incorrect field. This is because a message like “incorrect password” will help a hacker in knowing that the username is correct and he just needs to try a different combination on the password field only.
3. Verify the login session timeout duration. So, that once logged-in a user cannot be authenticated for a life-time.
4. Verify that once logged in, clicking the back button doesn’t logout the user.

**User profile Functionality:**

1. After changing password either through super user or normal user ,that

should properly reflected i.e user can login with new password only.

**Must to be covered functional areas:**

**Login Functionality:**

1. Verify that the user is not able to login with an invalid username and password.
2. Verify that the validation message gets displayed in case the user leaves the username or password field as blank.
3. Verify that the validation message is displayed in the case the user exceeds the character limit of the user name and password fields.
4. Verify that reset button functionality on the login page. Clicking on it should clear the textbox’s content.

**Environments :**

QC,UAT and Pre-prod

**Test Deliverable:**

* Test strategy
* Test plan and estimation
* Test scenario
* Test cases and test data
* RTM
* Test summary report
* Test closure report
* Incident report

**E2E Tests Coverage considered for automation**

1.Create New User and validate details

2.Change password for new user and validate by logging in using the new password.