

# Software Test Plan (STP) - ATM System (Sample)

**Project:** Customer Relationship Management (CRM) System

**Version:** 1.0

**Authors:** <Rajesh Banginwar / Kavana H,Karthik S,Khushi Mahesh,Kaveri Sharma>

**Date:** 04-09-2025

**Status:** Sample / Draft

## 1. Introduction

**Purpose:** This document defines the comprehensive test plan for the Customer Relationship Management (CRM) System v1.0. It outlines the objectives, scope, strategy, resources, and schedule for all testing activities.

**Scope:** Testing will cover all core features of the CRM system, including campaign management, lead capture and qualification, sales pipeline management, support ticketing, customer data management, and the loyalty program. Hardware interfaces (beyond standard web clients) and the internal logic of third-party services like payment gateways or email providers are excluded from this scope.

**References:** RM SRS v1.0, Design Specifications v1.0, GDPR/PII Protection Laws , WCAG 2.1 AA Guidelines.

**Definitions:**

- **CRM:** Customer Relationship Management
- **RBAC:** Role-Based Access Control
- **MFA:** Multi-Factor Authentication
- **PII:** Personally Identifiable Information
- **SLA:** Service Level Agreement

## 2. Test Items

- Authentication and RBAC Module
- Customer Data Management Module
- Campaign Management Module
- Sales & Opportunity Management Module
- Communication & Case Management Module
- Loyalty Program Module (Points, Tiers, Rewards)
- System Administration and Monitoring Interface

## 3. Features to be Tested

- CRM-F-001: User login via username/password with Role-Based Access Control.
- CRM-F-005: Adding new customer records with personal and business details.
- CRM-F-009: Creation of sales opportunities linked to customer records.
- CRM-F-013: Creation and tracking of support cases with SLA deadlines.
- CRM-NF-001: System performance to handle 500 concurrent users with <3s response time.
- CRM-NF-002: System reliability to provide 99.9% monthly uptime.
- CRM-N-005: System accessibility compliance with WCAG 2.1 AA standards.

## 4. Features Not to be Tested

- Internal logic of third-party email/SMS providers.
- The internal processing systems of payment gateways.
- External ERP/Accounting system logic beyond the defined API interactions.

## 5. Test Approach / Strategy

A multi-layered testing strategy will be employed to ensure comprehensive quality assurance.

- Levels:
  - Unit Tests: To verify individual components and functions.
  - Integration Tests: To validate interactions between CRM modules and third-party APIs (e.g., Email, E-Sign).

- System Tests: To conduct end-to-end testing of the complete, integrated system.
  - Acceptance Tests (UAT): To be performed by stakeholders to confirm the system meets business requirements.
- Types:
  - Functional Testing: To verify all core features listed in the SRS.
  - Security Testing: To validate authentication, authorization, and data protection measures.
  - Performance Testing: To test system responsiveness and scalability under load.
  - Usability & Accessibility Testing: To ensure the user interface is intuitive and compliant with WCAG 2.1 AA.
  - Regression Testing: To ensure new changes do not negatively impact existing functionality.
- Entry Criteria: A stable build is delivered to QA, the test environment is fully configured, and all necessary test data is available.
- Exit Criteria: 100% of planned test cases are executed, there are no open critical defects, and all high-priority acceptance criteria from the SRS have been met.

## 5.1 Security Validation

- Verify that TLS 1.2+ is enforced for all network connections.
- Confirm all customer data at rest is encrypted using AES-256 or equivalent.
- Test that RBAC is strictly enforced across all modules, preventing unauthorized access.
- Validate the MFA implementation for admin and manager roles.
- Ensure all security-related events are logged and retained as per compliance requirements.

## 6. Test Environment

Hardware: Standard web client machines. No specialized hardware is required.

Software: Modern web browsers (Chrome, Firefox, Safari), Linux container environment, relational database sandbox, and API sandboxes for third-party integrations (Email, SMS, Payments).

Tools: Selenium for UI automation, Postman for API testing, JMeter for performance testing, and Jira for defect tracking.

Test Data: A prepared set of dummy data including customer profiles, sales leads, opportunities, support cases, and marketing campaigns.

## 7. Test Schedule

Milestones:

- Test case design: 05-Sep-2025 - 09-Sep-2025

- Environment setup: 08-Sep-2025 - 11-Sep-2025
- Test execution start: 12-Sep-2025
- Test execution end: 03-Oct-2025
- UAT: 06-Oct-2025 - 10-Oct-2025

## 8. Test Deliverables

- Test Plan (this document)
- Test Cases (manual & automated)
- Test Scripts
- Test Data
- Test Execution Logs
- Defect Reports
- Test Summary Report

## 9. Roles and Responsibilities

Role	Name	Responsibility
QA Lead	<Karthik S>	Prepare plan, coordinate execution
Test Engineer	<Khushi Mahesh>	Design & execute test cases, log defects
Developer	<Kavana H>	Support defect fixes and triage
Product Owner	<Kaveri Sharma>	Approve test results, sign-off readiness

## 10. Risks and Mitigation

Risk	Mitigation
Delay in stable build delivery	Request early smoke builds from dev team
Test environment downtime	Maintain backup environment on cloud VM
Dependency on third-party ATM hardware vendor	Engage vendor early and maintain test stubs
Resource unavailability (QA/Test Engineers)	Cross-train team members and maintain a buffer in schedule.

## 11. Assumptions & Dependencies

Test data for customers, leads, and opportunities will be prepared and shared before execution.

- All required API stubs (Email, Payment, SMS) will be available and stable during testing.
- Core system modules will be delivered in integration-ready state.
- Required tools (Selenium, JMeter, Postman, Jira) will be licensed and accessible.
- Test environment will mimic production in terms of configuration and scalability.

## 12. Suspension & Resumption Criteria

Suspend testing if:

- Environment unavailable for >4 hours
- Build is too unstable (blocks >30% test cases)

Resume testing if:

- Blocking defects are resolved
- Environment stabilized

## 13. Test Case Management & Traceability

RTM ensures mapping of SRS requirements to test cases.

Example:

- ATM-F-001 (PIN validation) → TC-Auth-01, TC-Auth-02
- ATM-F-010 (Withdrawal) → TC-WD-01, TC-WD-02
- ATM-NF-001 (Response time) → TC-Perf-01

## 14. Test Metrics & Reporting

Metrics collected:

- % test cases executed
- % passed/failed
- Defect density
- Defect aging
- Requirement coverage

Reports:

- Daily execution status
- Final Test Summary Report

## 15. Approvals

Role	Name	Signature / Date
------	------	------------------

QA Lead		
Dev Lead		
Product Owner		

## 16. Test Cases

This section provides sample test cases for the ATM System. Each test case includes a unique identifier, description, preconditions, input data, expected results, and postconditions.

Test Case ID	Test Scenario / Description	Preconditions	Test Steps / Input Data	Expected Result	Postconditions / Remarks
Sprint 1					
TC-AUTH-01	Validate successful login (User)	A standard 'User' role account exists (e.g., user@crm.com, pass: P@ssword123) [Ref: CRM-F-001]	1. Navigate to the login page.  2. Enter email: 'user@crm.com'.  3. Enter password:	The user is redirected to the main dashboard. The navigation bar shows user-level items (no 'Admin	A secure session token (JWT) is created. Login attempt is logged as 'success'.

			<p>P@ssword123.</p> <p>4. Click 'Login'.</p>	Panel').	
TC-AUTH-02	Validate failed login (Wrong Password)	An 'Admin' role account exists (e.g., admin@crm.com) [Ref: CRM-F-001]	<p>1. Navigate to the login page.</p> <p>2. Enter email: 'admin@crm.com'.</p> <p>3. Enter password: WrongPassword.</p> <p>4. Click 'Login'.</p>	An error message "Invalid email or password" is displayed. The user remains on the login page.	Failed login attempt is logged [Ref: CRM-F-004].
TC-RBAC-01	Validate Admin role access	The user is logged in as 'Admin' (admin@crm.com). [Ref: CRM-F-001]	<p>1. After logging in, locate the 'Admin Panel' or 'User Management' link in the navigation.</p> <p>2. Click the link.</p>	The 'Admin Panel' page loads successfully, showing options to manage user roles and system	Access is granted per RBAC rules.

				settings.	
TC-RBAC-02	Validate User role restriction	User is logged in as 'User' (user@crm.com) . [Ref: CRM-F-001]	1. Attempt to navigate directly to the admin URL (e.g., /admin/settings).	The user is redirected to the dashboard or an "Access Denied" (403) page. The admin link is not visible.	Access is correctly denied per RBAC rules.
TC-CUST-01	Create new customer (Valid Data)	The user is logged in as 'Sales Rep' or 'Admin'. [Ref: CRM-F-005]	<p>1. Navigate to 'Customers' -&gt; 'Add New Customer'.</p> <p>2. Fill in all required fields (e.g., Name: 'John Doe', Email: 'john.doe@email.com', Phone: '555-1234').</p> <p>3. Click 'Save'.</p>	A success message "Customer John Doe created" is displayed. The user is redirected to the customer list or the new customer's profile.	A new customer record exists in the database. Audit trail is created [Ref: CRM-F-006].

TC-SUP-01	Log new support ticket	The user is logged in as 'Support Agent'. A customer (e.g., 'John Doe') exists. [Ref: CRM-F-013]	<p>1. Navigate to 'Support Tickets' -&gt; 'Create Ticket'.</p> <p>2. Select 'John Doe' from the customer search.</p> <p>3. Enter Subject: 'Login Issue'.</p> <p>4. Enter Description: 'User cannot log in'.</p> <p>5. Set Priority: 'High'.</p> <p>6. Click 'Submit'.</p>	A new ticket is created with a unique ID (e.g., TCK-1001) and appears in the support queue. The ticket is linked to 'John Doe'.	The ticket is saved in the database.
<b>Sprint 2</b>					

TC-AUTH-03	Validate successful login with MFA (Admin)	An 'Admin' account (admin@crm.com) has MFA enabled. [Ref: CRM-F-003]	<p>1. Enter email 'admin@crm.com' and correct password.</p> <p>2. Click 'Login'.</p> <p>3. On the 'MFA Verification' screen, enter the correct 6-digit OTP from the authenticator app.</p> <p>4. Click 'Verify'.</p>	The user is successfully logged in and redirected to the admin dashboard.	A secure, MFA-verified session is created.
TC-CUST-02	Prevent duplicate customer creation	The user is logged in. A customer with email 'john.doe@email.com' already exists. [Ref: CRM-F-007]	<p>1. Navigate to 'Customers' -&gt; 'Add New Customer'.</p> <p>2. Enter Name: 'Johnny Doe'.</p> <p>3. Enter Email: 'john.doe@email.com'.</p>	An error message "A customer with this email already exists" is displayed. The new customer is not created.	Duplicate record is blocked.

			4. Click 'Save'.		
TC-SUP-02	Verify SLA Deadline assignment	The user is logged in. SLA rules are configured (e.g., 'High' Priority = 4-hour deadline). [Ref: CRM-F-013]	<p>1. Create a new support ticket with 'High' priority (see TC-SUP-01).</p> <p>2. Open the newly created ticket.</p> <p>3. View the ticket details.</p>	The ticket details display an 'SLA Due' or 'Respond By' time that is 4 hours from the ticket's creation time.	SLA deadline is correctly calculated and stored.
TC-SUP-03	Verify SLA notification (mock)	A 'High' priority ticket's SLA is 1 hour from expiring. [Ref: CRM-F-014]	<p>1. (Test environment setup) Manually set a ticket's SLA to expire in 1 minute.</p> <p>2. Wait for the system's notification job to run.</p>	An email or in-app notification is sent to the assigned Support Agent or Manager (e.g., "Ticket TCK-1001 is approaching SLA breach").	Notification is logged as sent.

TC-UI-01	Verify Dashboard Skeleton load	User is logged in. [Ref: CRM-NF-001]	1. Navigate to the main 'Dashboard' page.	The dashboard page loads completely in under 3 seconds. All defined widgets (e.g., "My Open Tickets," "Sales Pipeline," "New Customers") are visible, even if they show "0" or "No data." No console errors.	Meets performance and basic UI requirements.
----------	--------------------------------	--------------------------------------	---	--	--