KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY,

KUMASI

INFORMATION SECURITY AND TECHNOLOGY ASSURANCE DIVISION, UITS.

User Acceptance Testing (UAT) Report and Execution Guide (ISO/IEC 27001)

PREPARED BY:

MR. STEPHEN KWADWO OSEI

MR. SIMON GOKA

MR. PHANUEL SELI KWADZO ASENSE

FEBRUARY 2025

Table of Contents

List of Tables

1. Introduction

User Acceptance Testing (UAT) is a critical phase in the software development lifecycle, where the application is tested by end users to ensure it meets business requirements and functions as expected. This report serves as a comprehensive guide for conducting UAT for the application interface. It outlines the objectives, requirements, and detailed instructions for performing and documenting UAT, with a strong emphasis on input and output validation.

---

2. Objectives

The primary objectives of this report are to:

- Provide clear and step-by-step instructions for conducting UAT.
- Ensure the application meets specified business, functional, non-functional, and security requirements.
- Validate input data to prevent errors and security threats.
- Verify that system outputs are accurate, consistent, and aligned with the defined requirements.
- Enable testers to identify and document issues, defects, and inconsistencies.

---

3. UAT Process Overview

The UAT process involves validating the application against predefined requirements. This section guides testers through the process.

3.1 Test Preparation:

- Identify the test environment and ensure it matches the production environment.
- Gather all required test data and documentation.
- Assign roles and responsibilities for testers.

3.2 Test Execution:

- Follow the detailed requirements provided in this manual.
- Document observations and results for each requirement.
- Conduct input and output validation at every step.
- Report any defects or issues identified.

3.3 Test Closure:

- Summarize test results and findings.
- Obtain sign-off from stakeholders.
- Prepare a final UAT report for submission.

4. Functional Requirements

Functional requirements specify what a system or software application must do to meet the needs of its users. These requirements focus on the specific behaviour and functions of the system.

NB: Requirements must be clearly defined and provided by the Software Development Division (SDD-UITS).

The following functional requirements outline generalized key operational functionalities that must be validated during UAT.

Table 1: Generalized Functional Requirements

Requirement ID	Description (Core Functional Operation & UI/UX Focus	Acceptance Criteria	Validation Focus (Generalized for any System)
001 User Authentication	The system should provide a secure, easy-to-use login mechanism with intuitive feedback.	User successfully logs in and receives appropriate error messages for failed attempts.	Ensure input sanitization, session management, and user feedback on login success/failure.
002 Password Management	Users should be able to reset and manage their passwords securely.	Password reset process is simple, and emails are received as expected	Validate email input format, reset link functionality, and expiration time.
003 Navigation & Menu System	The interface should be intuitive, with a clear navigation structure	Users can easily find and access all major system features.	Ensure menu items are logically grouped, with consistent navigation paths.
004 Data Entry Forms	Forms must be user-friendly, with validation for all fields.	Data is entered accurately, and incorrect inputs trigger appropriate error messages.	Validate input type, required fields, and maximum length constraints

005 Notifications & Alerts	The system should provide real-time notifications and alerts.	Users receive alerts for important events without delay.	Test for notification accuracy, timeliness, and user acknowledgment.
006 Requirements specific to system being developed	[Specific user requirements of the system under development/testing] [To be supplied by Software Development Division] [Derived from the user requirement document]		

5. Non-Functional Requirements

Non-functional requirements (NFRs) define how a system should perform rather than what it should do. They describe the quality attributes, constraints, and overall behaviour of the system, ensuring it meets performance, security, usability, and other operational standards. Unlike functional requirements, which focus on specific features, NFRs address the system's overall characteristics and user experience

Table 2: Non-Functional Requirements (NFR)

Requirement ID	Description	Acceptance Criteria	Validation Focus
001 System Performance	Application responds within acceptable time limits	Response time within specified thresholds	Output validation: performance metrics accuracy
002 Scalability	Application supports increasing concurrent users	Performance degradation under load must be within acceptable limits	Output validation: consistent behaviour under load
003 Reliability	Application remains stable during prolonged use	No crashes or unexpected downtime	Output validation: confirm stability through logs
004 Compatibility	Application works across different devices and browsers	Full functionality maintained across platforms	Output validation: multiple device/browser comparison
005 Accessibility	Complies with WCAG 2.1 standards (Web Content Accessibility Guidelines 2.1)	Accessible to users with disabilities	Output validation: compliance with accessibility requirements

6. Security Requirements (SR)

Security requirements ensure the application is protected from vulnerabilities and unauthorized access.

Requirement 1: Data Encryption

- Description: All sensitive data must be encrypted during transmission and at rest.
- Acceptance Criteria: Data is secured using TLS 1.2/1.3 for transmission. Strong encryption at rest for sensitive data as may be required.
- Output Validation: Verify encrypted data storage.

Requirement 2: Cross-Site Scripting (XSS) Prevention

- Description: The application must prevent XSS attacks through input validation and content security policies.
- Acceptance Criteria: No XSS vulnerabilities are found during testing.

Requirement 3: SQL Injection Protection

- Description: Input fields must be protected against SQL injection attacks.
- Acceptance Criteria: SQL injection attempts are blocked.

Requirement 4: Multi-Factor Authentication (MFA)

- Description: The application must implement MFA for enhanced security.
- Acceptance Criteria: MFA is available and enforced for all users.

Requirement 5: Secure Session Management

- Description: Sessions must be managed securely with appropriate timeout and cookie policies.
- Acceptance Criteria: Session cookies are secure, and sessions time out after inactivity.

7. Documentation and Reporting

Each tester must document their findings using the provided templates. Documentation should include input and output validation steps.

7.1 Input Validation Documentation:

- Specify the data type, range, and format expected for each input field.
- Record values tested and any errors encountered.

7.2 Output Validation Documentation:

- Compare output with expected results.
- Document any inconsistencies or anomalies.

7.3 Defect Reporting:

- Requirement ID and description.
- Steps performed.
- Observations and results.
- Defects or issues identified.

---

8. Recommendations

On completing the UAT, the following steps should be taken:

1. Review and address all identified issues (by the division responsible).
2. Ensure that all requirements have been validated successfully.
3. Prepare a summary report with recommendations.
4. Obtain final sign-off from stakeholders.

---

9. Appendix

Template for UAT Compliance

Table 3: Functional Requirements to be filled in by Software Development Team

Requirement ID	Requirement Title	Requirement Description	Acceptance Criteria	Compliance Status (Yes/No)	Remarks	Date
FR-001						
FR-002						
FR-003						
FR-004						
FR-005						
FR-006						
FR-007						

Table 4: UAT template for Non-functional requirement

Requirement ID	Description	Compliance Status (Yes/No)	Remarks	Date
NFR-001	System Performance			
NFR-002	Scalability			
NFR-003	Reliability			
NFR-004	Compatibility			
NFR-005	Accessibility			

Table 5: UAT template for Security requirement

Requirement ID	Requirement Description	Acceptance Criteria	Compliance Status (Yes/No)	Remarks	Date
SR-001 Data Encryption	All sensitive data must be encrypted during transmission and at rest	Data is secured using TLS 1.2/1.3 for transmission and strong encryption at rest.			
SR-002 Cross-Site Scripting (XSS) Prevention	The application must prevent XSS attacks through input validation	No XSS vulnerabilities are found during testing.			

	and content security policies.				
SR-003 SQL Injection Protection	Input fields must be protected against SQL injection attacks	SQL injection attempts are blocked.			
SR-004 Multi-Factor Authentication (MFA)	The application must implement MFA for enhanced security.	MFA is available and enforced for all users.			
SR-005 Secure session Management	Sessions must be managed securely with appropriate timeout and cookie policies.	Session cookies are secure, and sessions time out after inactivity.			

Approval & Sign-off

UAT Coordinator: ....

Date: ....

Stakeholder(s): ....
....

....

....

Date: ....