Mobile Application Security Testing Requirements Document

Prepared By:

Information Network Security Administration (INSA)

2025

Submitted by:

[Client's Name / Organization]

Submitted to:

Information Network Security Administration (INSA)

Cyber Security Audit Division Wollo Sefer, Addis Ababa, Ethiopia

Contact Person:

Tilahun Ejigu (Ph.D.)

Cyber Security Audit Division Head

✉: tilahune@insa.gov.et

📱: +251 937 456 374

Submission Date: [Insert Date]

Due Date for Response: Within Five (5) Working Days from the Date of Receipt

1. Background of INSA

The Information Network Security Administration (INSA) is Ethiopia's leading government body entrusted with safeguarding the country's digital infrastructure and cyber ecosystem. Established with a vision to ensure national cyber sovereignty and resilience, INSA performs critical functions such as conducting cyber security audits, providing policy direction, issuing compliance guidelines, and offering technical support across various governmental and private institutions.

INSA's Cyber Security Audit Division assesses the security posture of digital platforms including web applications, APIs, mobile applications, internal portals, and IT infrastructures. Our assessments identify vulnerabilities and recommend mitigation strategies aligned with global best practices.

2. Introduction

This document outlines the key requirements and submission expectations for organizations undergoing mobile applications security testing with INSA. The aim is to ensure robustness, confidentiality, and integrity of digital assets by identifying and addressing vulnerabilities. INSA applies leading methodologies and standards including OWASP Top 10, NIST guidelines, and ISO/IEC 27001.

3. Mobile Application Security Audit Requirements

3.1 Business Architecture and Design / Ecosystem of Mobile Applications (Mandatory)

To initiate a mobile application security audit, the requesting organization **must** provide the following information and documentation:

1. Business Architecture and Design

- You **must** submit a detailed description of the business architecture and design of the mobile application.

- It **should** include the purpose, goals, main services, user types, and core processes supported by the application.

2. Data Flow Diagram

- You **must** provide a complete data flow diagram (DFD) that shows how data moves between users, the mobile app, backend services, and external systems.
- The diagram **should** clearly define sensitive data entry points, data storage, and transmission channels.

3. System Architecture Diagram with Database Relation

- You **must** submit a system architecture diagram that explains the application layers, backend servers, APIs, and integrations.
- It **should** include database relations, schemas, and key data entities with their relationships.

4. Native Applications

- If the mobile application is native (Android/iOS), you **must** specify the development framework, programming languages, SDKs, and versions used.
- You **should** also provide platform-specific security features and libraries applied.

5. Hybrid Applications

- If the application is hybrid, you **must** document the framework (e.g., React Native, Flutter) and supporting plugins.
- You **should** provide details on how native and web components interact within the app.

6. Progressive Web Apps (PWA)

- If the application is a PWA, you **must** describe its deployment method, supported browsers, and offline capabilities.
- You **should** indicate how caching, service workers, and push notifications are implemented.

7. Threat Model Mapping

- You **must** submit a threat model mapping that identifies possible attack vectors (e.g., injection, insecure storage, broken authentication).
- It **should** outline the applied security controls and risk mitigation measures.

8. System Functionality

- You **must** describe all key functionalities of the mobile application, including authentication, payments, notifications, and integrations.
- You **should** highlight security-critical features such as financial transactions, sensitive data handling, or third-party APIs.

9. Role / System Actor Relationship

- You **must** provide a role-based access control (RBAC) model that maps system actors (users, admins, merchants, agents, etc.) to their permissions.
- You **should** explain restrictions applied to enforce least privilege and separation of duties.

10. Test Account

- You **must** provide at least one functional test account (user and admin, if applicable) with all required credentials and permissions.

- The account **should** include test data that mirrors real-world usage without exposing actual sensitive customer data.

11. Source Code & Build Files (If Required for Audit)

- You **must** provide the mobile application's latest build file (.apk for Android, .ipa for iOS).
- You **should** provide the source code or selected modules if required for deeper code review.

12. API Documentation & Access

- You **must** submit updated API documentation including endpoints, authentication, and response structures.
- You **should** provide test API keys and tokens for integration testing.

13. Third-Party Services & SDKs

- You **must** list all third-party services, libraries, and SDKs integrated into the application.
- You **should** include details of security measures for each (e.g., payment gateways, analytics tools).

14. Authentication & Authorization Details

- You **must** provide documentation of authentication mechanisms (password, biometrics, OAuth, tokens).
- You **should** submit details of session management and authorization controls.

15. Compliance & Regulatory Requirements

- You **must** declare compliance obligations relevant to the app (e.g., PCI DSS, local laws)
- You **should** provide internal security policies or standards applied.

16. Secure Communication Details

- You **must** document encryption methods (SSL/TLS, certificate pinning, data-at-rest protection).
- You **should** specify key management practices and protocols in use.

17. Logging & Monitoring Setup

- You **must** explain how the application logs user activity and security events.
- You **should** include details of monitoring and alerting systems.

Table 1: Summary For The Above Requirements

Business Architecture and Design	**You must provide this information (Mandatory)**
Data Flow Diagram	**(Mandatory)**
System Architecture Diagram with data base relation	**(Mandatory)**
Native Applications	**(Mandatory)**
Hybrid Applications	**(Mandatory)**
Progressive Web Apps (PWA)	**(Mandatory)**
Threat Model Mapping	**(Mandatory)**
System Functionality	**(Mandatory)**
Role / System Actor Relationship	**(Mandatory)**
Test Account	**(Mandatory)**

2. Purpose and Functionality of the Mobile Application (Mandatory)

1. OS Supported by the Mobile Application

- The customer **must** specify the operating systems supported (Android, iOS, or both).
- The customer **should** include the minimum and maximum OS versions supported.

2. Source Code or Binary (APK/IPA)

- The customer **must** provide the latest application binary (.apk for Android, .ipa for iOS).
- If required, the customer **should** provide access to the source code or selected modules for in-depth static analysis.

3. Specific Functionalities or Components for Detailed Testing

- The customer **must** identify application components or features that require detailed testing (e.g., login, payment, file upload).
- The customer **should** highlight security-critical workflows that handle sensitive or financial data.

4. Compliance or Security Requirements

- The customer **must** declare compliance obligations applicable to the application (e.g., PCI DSS, GDPR, PSD2, local data protection laws).
- The customer **should** provide internal security standards or policies followed in development.

5. Authentication Mechanisms Used

- The customer **must** provide details of authentication mechanisms (e.g., password-based, biometrics, OTP, OAuth2, token-based).
- The customer **should** include session management and account recovery methods.

6. Sensitive Data Stored or Transmitted

- The customer **must** disclose any sensitive data types stored or transmitted by the application (e.g., PII, financial details, location, health records).

- The customer **should** specify data retention and transmission channels used.

7. Handling of Sensitive Data

- The customer **must** describe how sensitive data is secured (encryption, masking, secure storage APIs).
- The customer **should** provide details on key management practices and data protection mechanisms.

8. Integration with Third-Party Services or APIs

- The customer **must** list all third-party integrations (e.g., payment gateways, social logins, analytics SDKs).
- The customer **should** provide documentation of security measures for each integration.

9. Restrictions or Limitations on Testing Approach

- The customer **must** state any restrictions on testing techniques (e.g., no denial-of-service, no live data tampering).
- The customer **should** provide guidelines for safe testing environments (e.g., sandbox or staging servers).

10. Known Vulnerabilities or Security Concerns

- The customer **must** provide details of any known vulnerabilities, past audit findings, or pending fixes.
- The customer **should** highlight security areas of concern that require additional attention.

Table 2: Summary of Purpose And Functionality Of The Mobile Application Requirements(Mandatory)

Some specific question for the mobile application	**You should provide this information**
OS Supported by the mobile Application	
Source code or binary (APK)	
Are there any specific functionalities or components of the mobile application that need to be tested in detail?	
Any specific compliance or security requirements that the mobile application must adhere to	
Authentication mechanisms used in the mobile application	
Are there any sensitive data stored or transmitted by the mobile application	
How the sensitive data has been handled within the application?	
Does the mobile application integrate with any third-party services or APIs?	
Are there any restrictions or limitations on the testing approach or techniques that can be used?	
Are there any known vulnerabilities or security concerns with the mobile application that need to be specifically addressed?	

3. Define the specific scope clearly and precisely like this table (Mandatory)

Name of the Assets to be Audit	APK/official link	Test Account as required by the tester
Static Analysis		
Dynamic Analysis		
Automated Source Code Analysis		

4. Your Contact information and communication channel

Name	Role	Address (mail and Mobile)

5. Submission Instructions

Submit all materials via INSA's Audit Request Portal. For sensitive files (e.g., source code or APKs), deliver those on CD/DVD to INSA's office or mail them to:

Information Network Security Administration (INSA)

Cyber Security Audit Division Wollo Sefer, Addis Ababa, Ethiopia

Contact: Tilahun Ejigu (Ph.D.), Division Head

Email: tilahune@insa.gov.et

Mobile: +251 937 456 374

6. Conclusion

INSA is committed to working collaboratively to improve your organization's digital security posture. By submitting the required documentation within the specified timeline, you enable a comprehensive and accurate audit that enhances compliance, strengthens service delivery, and reduces exposure to cyber threats.

Note!! The document contained

1. **cover page and correct company name**
2. **background of organization**
3. **Introduction**
4. **Objective of this certificate requested**
5. **Conclusion**