# Security Compliance Assessment Report

**Client**: [redacted] (Fintech Startup)

**Assessment Type**: Security Compliance Gap Assessment

**Assessment Period**: August 1, 2024 – August 15, 2024

**Prepared by**: Shoumik Chandra – Cybersecurity Consultant

## Table of Contents

## Executive Summary

This assessment was conducted to review [redacted] adherence to essential security and compliance controls under the Cybersecurity Framework and ISO/IEC 27001. The objective was to identify key gaps and advise the organization on a roadmap to enhance compliance posture before their product launch.

## Scope & Objectives

- **In-Scope Systems**: Core fintech web app, internal APIs, authentication flow, infrastructure (AWS), third-party services (OTP gateway)
- **Compliance Scope**:
  - RBI guidelines (Data protection, KYC, authentication, access control)
  - ISO 27001 Annex A controls (Asset management, access control, incident response, etc.)

## Methodology

- Documentation Review (policies, configurations, user access)
- Interview with Tech Lead
- Light Penetration Testing (auth flow, data exposure)
- Compliance Checklist Mapping
- Risk-Based Gap Analysis

## Key Compliance Areas Reviewed

| Domain | Status |
|---|---|
| Data Encryption | Partially Compliant |
| Access Controls | Non-Compliant |
| Authentication & MFA | Compliant |
| Vendor Risk Management | Not Implemented |
| Logging & Monitoring | Partially Compliant |
| Data Retention & Disposal | Non-Compliant |
| Secure Development | No Secure SDLC Process |
| Incident Response | No Plan Available |

## Summary of Observations

| Compliance Domain | Severity | Description |
|---|---|---|
| Access Control | High | No role-based access segregation implemented |
| Vendor Risk Management | High | No contracts or risk assessments for 3rd parties |
| Logging & Monitoring | Moderate | No SIEM tool, logs not retained beyond 7 days |
| Secure Development | Moderate | No code review or secure coding guidelines |
| Data Disposal | Low | No documented data retention policy |

## Sample Detailed Finding

### Finding #1: Lack of Access Control Segregation

- **Standard Violated**: ISO/IEC 27001 – A.9.1.2
- **Impact**: Potential for privilege abuse by junior employees
- **Evidence**: [redacted]
- **Recommended Action**: Implement role-based access controls via IAM policies in AWS; restrict access by role and business need
- **Risk Rating**: High

### Finding #2: Absence of Third-Party Risk Assessment

- **Standard Violated**: RBI Guidelines – Para 2.2
- **Impact**: Exposure to supply chain threats
- **Evidence**: [redacted]
- **Recommended Action**: Formalize vendor onboarding and conduct risk assessments before integration
- **Risk Rating**: High

## Risk Rating Matrix

| Likelihood | Impact | Risk Level |
|---|---|---|
| Likely | High | High |
| Likely | Medium | Moderate |
| Unlikely | High | Moderate |

## Recommendations & Roadmap

| Priority | Control Area | Action Item | Timeline |
|---|---|---|---|
| High | Access Control | Define roles and implement IAM policies | 1 Month |
| High | Vendor Management | Document vendor onboarding checklist | 1 Month |
| Medium | Logging | Retain logs for 90 days + enable alerts | 2 Months |
| Medium | Secure Development | Introduce code review & training | 2 Months |
| Low | Data Retention Policy | Create and document disposal process | 3 Months |

## Appendix

**Tools Used**:

- Manual review
- AWS IAM Analyzer
- Burp Suite (auth flow inspection)
- Nessus Essentials
- Excel Compliance Checklist (customized for fintech)

**Documents Collected**:

- Privacy Policy
- Terms of Service
- AWS Architecture Diagram
- Employee Access Sheet

## Conclusion

The security compliance assessment of the fintech application environment reveals that while the organization has implemented several foundational controls aligned with best practices, there are notable gaps that must be addressed to achieve full alignment with financial regulatory frameworks and industry security standards like ISO 27001, SOC 2, and PCI DSS.

To strengthen the organization's compliance posture:

- Identified non-conformities should be remediated with high priority.
- Policies and procedures should be reviewed, formalized, and tested regularly.
- A recurring audit and continuous monitoring process should be established to maintain compliance in a dynamic threat landscape.

By addressing these issues, the organization will significantly reduce its risk exposure and move closer to a compliant, secure, and resilient operational state — vital for trust, customer retention, and successful long-term growth in the fintech sector.