Executive Summary

Project Title: Fintech Cybersecurity Risk Assessment
Environment: Simulated Mid-Sized Nigerian Fintech

---

1. Objective

The objective of this assessment was to identify, evaluate, and prioritize cybersecurity risks affecting a mid-sized fintech organization handling sensitive customer data and financial transactions. The assessment aimed to provide structured risk visibility and recommend practical mitigation strategies aligned with industry best practices.

---

2. Scope

The scope of this assessment included:

- Payment processing infrastructure
- Customer data management systems
- Cloud infrastructure
- Employee endpoints
- Third-party vendor integrations
- Backup and recovery systems

---

3. Methodology

A qualitative risk assessment methodology was applied using a Likelihood × Impact scoring model (1–5 scale).

Risk ratings were categorized as:

- Low (1–5)
- Medium (6–14)
- High (15–25)

The assessment approach aligns with principles outlined by:

- International Organization for Standardization ISO 27001 risk management framework
- National Institute of Standards and Technology NIST Cybersecurity Framework (Identify Function)

4. Key Findings

The assessment identified eight primary risks, with four classified as High Risk.

Top critical risks include:

1. SQL Injection vulnerability within the Payment API
2. Phishing exposure due to limited employee awareness
3. Cloud infrastructure misconfiguration
4. Inadequate vendor security due diligence

These risks pose potential impacts including financial fraud, regulatory penalties, reputational damage, and operational disruption.

---

5. Risk Treatment Strategy

Recommended mitigation strategies include:

- Implementation of Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC) enforcement
- Web Application Firewall (WAF) deployment
- Vendor security assessment program
- Endpoint Detection & Response (EDR) implementation
- Formalized cloud configuration governance

Residual risks were reassessed post-treatment and reduced to acceptable levels within defined risk appetite thresholds.

---

6. Conclusion

This assessment demonstrates the importance of proactive risk identification and structured governance in fintech environments. By implementing the recommended controls, the organization significantly reduces exposure to operational, financial, and regulatory risks while strengthening its overall security posture.