Shomar Security Platform

A CyberCapSec LTD product

PCI-DSS Readiness Guide for Nigerian Fintechs

Practical readiness guide for cardholder data, payment gateways, and secure SDLC

Audience

Payment gateways, PSPs, switches, merchants, processors, fintechs, and engineering teams that touch cardholder data.

Shomar Security Platform is a CyberCapSec LTD product for security operations, compliance evidence management, and regulated technology teams.

This resource is provided for planning and readiness support. It is not legal, regulatory, or audit attestation advice.

Purpose

PCI DSS readiness is easier when technical controls, evidence, vulnerability management, and ownership are handled continuously instead of shortly before an assessment.

Scope and architecture

- Document cardholder data environment boundaries.
- Maintain network diagrams and data flow diagrams.
- Confirm segmentation approach and test segmentation effectiveness.
- Track all systems that store, process, or transmit cardholder data.
- Maintain inventory of third-party payment services and responsibilities.

Core security controls

- Harden systems and remove unnecessary services.
- Encrypt sensitive data in transit and at rest where required.
- Use MFA for administrative and remote access.
- Centralise logs and review security events.
- Patch systems and remediate high-risk vulnerabilities quickly.

Secure SDLC and testing

- Run SAST, dependency, secrets, container, and IaC scans before release.
- Track critical and high findings to closure.
- Run ASV scans and penetration tests as required by scope.
- Document secure coding training and release approval gates.
- Keep evidence of retesting after remediation.

How Shomar helps

- Maps scanner findings and evidence to PCI DSS control areas.
- Tracks remediation tasks, owners, due dates, and retests.
- Supports reports for assessors, executives, and internal governance.
- Keeps payment-security readiness visible between formal audits.