Shomar Security Platform

A CyberCapSec LTD product

How Shomar Helps Microfinance Banks Comply with CBN Cybersecurity Guidelines

Compliance mapping guide for MFB cyber governance, CSAT readiness, evidence, and remediation

Audience

Microfinance bank boards, MD/CEOs, compliance managers, internal auditors, IT leads, and service providers supporting Nigerian MFBs.

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.

Regulatory context

Microfinance banks should treat CBN cybersecurity expectations as an operating discipline, not as a once-a-year document pack. The 2022 Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions set minimum expectations for OFIs, while the 2026 CBN Cybersecurity Self-Assessment Tool made fresh, evidence-backed self-assessment a supervisory focus across banks and selected OFIs.

This guide shows how Shomar can help an MFB translate those expectations into assigned controls, technical testing, remediation tasks, and management-ready proof.

- Cybersecurity governance and senior management oversight.
- Cybersecurity risk management and current risk treatment plans.
- Operational resilience, backup, recovery, and incident readiness.
- Metrics, monitoring, reporting, and evidence freshness.
- Technology, third-party, access, and vulnerability control evidence.

Compliance mapping model

Shomar starts with a scoped MFB framework bundle. Each obligation becomes owned work, and each piece of evidence can be linked to the relevant control area instead of being copied across disconnected spreadsheets.

- Governance maps to policy approval, role assignment, management reports, board packs, and review cadence.
- Risk management maps to risk registers, asset criticality, treatment plans, exceptions, and residual risk notes.
- Operational resilience maps to incident playbooks, escalation contacts, tabletop evidence, backup tests, and recovery exercises.
- Technology controls map to access reviews, MFA coverage, endpoint and cloud configuration, logging, vulnerability scans, and retests.
- Third-party controls map to vendor inventories, due diligence evidence, contracts, service reviews, and outsourced technology risk.

Evidence MFB teams should keep live

A lean MFB does not need a heavy enterprise GRC programme to start. It needs a controlled evidence trail that shows what exists, who owns it, when it was reviewed, and what changed after gaps were found.

- Approved cybersecurity policy, information security policy, and acceptable-use rules.
- Cybersecurity owner, escalation matrix, and management reporting evidence.
- Asset inventory covering endpoints, core banking systems, internet-facing services, cloud systems, and key vendors.

- Access review, privileged access review, MFA status, and joiner-mover-leaver evidence.
- Vulnerability scan or VAPT report with remediation owners, due dates, exceptions, and retest proof.
- Incident response playbook, tabletop exercise notes, incident register, and regulator notification workflow.
- Backup and recovery test evidence for critical customer, transaction, and reporting systems.

How Shomar supports the operating workflow

Shomar turns MFB cybersecurity readiness into a repeatable loop that compliance, IT, audit, and leadership can all follow.

- Scope: assign the MFB compliance bundle and confirm applicable cybersecurity, privacy, AML, and operational evidence lanes.
- Assess: record current evidence, identify missing controls, and create gaps with priority and owner.
- Test: run approved application, API, exposure, dependency, cloud, or VAPT workflows where relevant to the MFB environment.
- Remediate: link findings to controls, assign owners, track due dates, and record exceptions with approval and expiry.
- Prove: retake assessments, attach retest evidence, and export executive, audit, or CSAT-readiness summaries.

Technical controls Shomar can evidence

Where configured for the customer environment, Shomar helps an MFB connect technical security activity to compliance evidence rather than leaving scanner results in a separate tool.

- Application, API, dependency, secrets, container, and IaC scan history.
- External exposure and VAPT findings with severity, asset context, owner, remediation status, and retest evidence.
- Control mappings that connect findings to CBN-aligned cybersecurity obligations.
- Evidence freshness tracking so stale documents are visible before management or regulatory review.
- Customer-owned evidence storage patterns for sensitive documents where policy requires local control.

Practical CSAT readiness pack

For a CSAT-style submission or supervisory review, Shomar can help the MFB assemble a clear pack that shows both current posture and remediation progress.

- Cybersecurity governance summary and named accountability.
- Risk register, top cyber risks, treatment plan, and residual risk view.
- Technology and third-party control evidence with current status.
- Incident response and operational resilience evidence.
- Open gaps, remediation owners, target dates, exceptions, and retest status.
- Executive summary suitable for management, board, internal audit, or external adviser review.

Reference notes

- CBN circular dated 29/06/2022: Letter to all OFIs on the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions.
- CBN circular dated 30/03/2026: Deployment of Cybersecurity Self-Assessment Tool (CSAT).
- CBN Reforms and Initiatives page: CSAT summary for regulated financial institutions.

Important note

This guide is for planning and readiness support. It is not legal, regulatory, audit, or supervisory advice. Each MFB should confirm its exact obligations, licence conditions, and submission expectations with qualified advisers and the relevant regulator-facing officials.