

SHOMAR SECURITY PLATFORM

Enterprise Operations Pack

Procurement and implementation checklist for bank-grade Shomar deployment.

Document Control

Audience: Procurement, risk, technology, security, compliance, audit, and executive stakeholders

Classification: Customer-facing procurement support

Generated: August 01, 2026

Website: <https://shomar.io>

Application: <https://app.shomar.io>

Shomar is a security and compliance evidence platform for regulated Nigerian and African teams. It combines security scanning, findings operations, compliance evidence, customer-controlled scanning, and auditor-ready reporting in one operating workspace.

Contents

No.	Section
1	Enterprise Operations Pack Contents
2	Bank Readiness Claims
3	Implementation Checklist

1. Enterprise Operations Pack Contents

This pack is the shareable buyer and implementation bundle for banks, fintechs, auditors, and procurement reviewers evaluating Shomar at enterprise scale.

Artifact	Purpose	Owner
MCP Agent Operations Guide	Shows how agents safely read, plan, report, remediate, and operate through Shomar.	Platform admin
Enterprise Capacity Proof	Shows how Shomar supports multiple clients, projects, developers, and concurrent scans.	Platform operations
Vendor Procurement Pack	Provides VSQ, architecture, encryption, MFA, RBAC, logging, and API security answers.	Compliance/procurement
RBAC Architecture	Maps roles to permissions and page access.	Org admin
VAPT Authorization Guide	Documents verified scope, ROE, scan windows, rate limits, and retest flows.	Security officer
Evidence Vault Proof	Shows checksum, source hash, retention, and signature verification.	Compliance/audit

2. Bank Readiness Claims

Shomar can support a client with 10 projects and several developers when the organization has correctly configured projects, roles, API keys, quotas, scan windows, and worker pools.

At multi-client scale, the correct operating claim is not unlimited scanning. The correct claim is governed concurrency with tenant quotas, queue visibility, worker-pool controls, evidence output, and autoscale recommendations.

Procurement wording

Shomar supports multi-project, multi-developer, multi-client security and compliance operations through tenant isolation, scoped API keys, queue management, worker pools, enterprise quotas, incremental reruns, evidence vaulting, and auditable MCP automation.

Question	Short answer
Can one client scan 10 projects?	Yes, subject to project setup, source authorization, scan type, quotas, and worker capacity.
Can developers scan from CI/CD?	Yes. CI/CD keys can trigger scans, check status, download evidence, and rerun incrementally.
Can compliance teams use the same platform?	Yes. Evidence, gaps, frameworks, questionnaires, reports, and audit packs are organization-scoped.
Can 10 clients use Shomar at once?	Yes, with tenant quotas, worker pools, queue monitoring, autoscale recommendations, and production sizing.
Will scans drag the platform?	The platform monitors queue depth, saturation, p95 agent latency, and worker capacity so operators can throttle or scale.

3. Implementation Checklist

Use this checklist before announcing a bank-ready pilot or production launch.

Area	Required control
Organization	Users, roles, departments, projects, and license are configured.
API keys	Separate IDE, CI/CD, reporting, compliance, and enterprise MCP keys exist with constraints.
Scans	Incremental scan, full scan, retest, and VAPT queues are tested.
VAPT	Verified scope, ROE approval, test window, rate limit, and stop conditions are enforced.
Compliance	Frameworks, evidence mappings, gaps, questionnaires, and reports are active.
Connectors	Source control, ticketing, SIEM, productivity, and evidence connectors are monitored.
Observability	Enterprise Ops and Agent Ops show queue, worker, p95 latency, failures, approvals, and connectors.
Procurement	VSQ, architecture diagram, RBAC PDF, MCP guide, and capacity proof are ready to share.