ASSESS ONCE · EVIDENCE EVERYWHERE

Every SBP requirement that applies to you. Assessed. Evidenced. In one workspace.

ETGRMF, AML/CFT, the Foreign Exchange Manual, digital banking and mobile app security, outsourcing and cloud, card security, Raast participation, the PS&EFT Act and the microfinance Prudential Regulations, broken into individual requirements you can assess, attach evidence to and report on, filtered to your entity type: bank, DFI, microfinance bank, digital bank, EMI, PSO or PSP.

1,504	17	7	5-day
requirements pre-loaded	SBP instruments covered	regulated entity types	free trial, no card

ONE REQUIREMENT AS LOADED — **MOBILE APPLICATIONS SECURITY GUIDELINES, SECTION 7E**

SBP MOBAPP-2022 | PSP&OD Circular 01/2022 | Network & session security

Applies to: bank · MFB · DFI · digital bank · EMI · PSO · PSP

REQUIREMENT

Enforce transport layer encryption between the app and all app servers and back-end services, with a trust manager of the owner's own that rejects unknown certificates, defences against bypassing certificate pinning, and no operation while certificate errors persist.

HOW TO TEST IT

Test the app against an intercepting proxy and invalid certificates.

CLAUSE

Section 7E(i) to (v).

SET A STATUS, ADD A NOTE AND ATTACH EVIDENCE ON THE ROW — AND SEE IT IN THE DASHBOARD AND THE BOARD REPORT.

Kim — I built this after years of running SBP circulars through a different spreadsheet for every instrument. It is designed, maintained and supported by me, from Pakistan. Questions before you start? Email me directly.

5-day free trial · Annual — $500 per seat, no minimum · kim_abdalian@yahoo.com

© 2026 KIM

THE PROBLEM

A folder of circulars, and a spreadsheet for each one.

SBP issues requirements across many circulars, frameworks and manuals. Each gets its own tracker, owned by a different person, updated at a different time. Nobody can say what applies to a microfinance bank and what applies to a payment provider without re-reading all of them, and the status is unknown the day before an inspection.

Today

Circulars as PDFs · a spreadsheet per instrument · evidence scattered across email and shared drives · a board paper rebuilt by hand every quarter.

With KSBPRC

Every requirement in one workspace, citing the circular and clause it came from, filtered to your entity type, with evidence attached to the requirement it proves.

WHAT CHANGES

01 Applicability by entity type

A microfinance bank is not asked to assess requirements written for a payment system operator. Tick your entity types once; the workspace shows only the instruments that apply.

02 Cited to the source

Every requirement names its instrument and clause, so nobody has to take our word for it. SBP's published texts always prevail.

03 Assessment scope per instrument

Record the purpose, start date and end date of each assessment; the report states scope and period per instrument.

04 Board-ready in minutes

A PDF and a CSV for any selection of instruments, with pie charts and a category roll-up. Add your logo, header title and footer line; they print on every page.

BUILT FOR

- ✓ **Banks and DFIs** — ETGRMF, AML/CFT, the FX Manual, digital banking security and the outsourcing and cloud frameworks in one place.
- ✓ **Microfinance banks** — the Prudential Regulations for MFBs, branchless banking and the 2023 digital banking measures.
- ✓ **Digital banks** — the licensing framework with the technology, outsourcing and onboarding requirements it relies on.
- ✓ **EMIs, PSOs and PSPs** — the Technology Risk Management Framework, Raast participation, mobile app security and the PS&EFT Act.
- ✓ **Consultancies and audit firms** — a separate workspace per client; read-only seats for reviewers; reports in your client's branding.

© 2026 KIM

SEVENTEEN INSTRUMENTS

1,504 requirements, drawn from SBP's own texts.

INSTRUMENT	REFERENCE	REQS
Enterprise Technology Governance & Risk Management Framework	BPRD Circular 05/2017	258
Outsourcing Risk Management Framework	BPRD Circular 06/2019	138
Cloud Outsourcing Framework	BPRD Circular 01/2023	128
Digital Banking Security	BPRD Circular 04/2023	96
Consolidated Customer Onboarding Framework	BPRD Circular 01/2025	75
Licensing & Regulatory Framework for Digital Banks	BPRD Circular 01/2022	67
Regulations for Payment Card Security	PSD Circular 05/2016	53
Cyber Shield — Cyber Resilience Strategy 2025-2030 (readiness)	CRMD Circular Letter 01/2026	26
Security of Digital Payments	PSD Circular 09/2018	20
AML/CFT/CPF Regulations for SBP Regulated Entities	BPRD Circular 05/2020	64
Branchless Banking Regulations	BPRD Circular 10/2019	111
Prudential Regulations for Microfinance Banks	ACFID Circular 01/2025	128
Payment Systems and Electronic Fund Transfers Act 2007	Act IV of 2007	62
Foreign Exchange Manual — Authorized Dealers	Exchange Policy Dept.	157
Raast Participation Criteria	PSP&OD Circular 01/2025	24
Mobile Applications Security Guidelines	PSP&OD Circular 01/2022	44
Technology Risk Management Framework for Payment Institutions	PSP&OD Circular 04/2025	53

The Cyber Shield strategy is tracked as direction of travel and kept apart from mandatory requirements, so the two are never confused in a board paper. The FX Manual applies to banks, DFIs and digital banks; the TRM Framework to EMIs, PSOs and PSPs; the MFB Prudential Regulations to microfinance banks. More instruments are added, from the official text and checked, as SBP issues them.

© 2026 KIM

TECHNICAL EVALUATION

The dashboard, and the review that fills it.

Every instrument opens with its own progress, a pie chart of statuses (full, partial, non-compliant, not applicable, not assessed) and a category roll-up. Every requirement has a status, a note and its own evidence, and the clause reference sits on the row. Nothing to configure: the library ships loaded.

THE REVIEW, IN FOUR STEPS

01 Set your entity types

Settings → Regulated entity type. The workspace lists only the instruments addressed to those types.

02 Set the scope

Per instrument: purpose, start and end date. Reports carry them.

03 Assess and evidence

Status, owner note and an attached file on each requirement; owners, editors and viewers, with an audit trail of every change.

04 Export the report

Pick instruments, add the client name and logo, download the PDF; CSV for the workpapers; an evidence pack as a ZIP with a manifest.

INCLUDED

- ✓ Requirements taken from SBP's own circulars, each citing its instrument and clause
- ✓ Applicability by entity type: bank, microfinance bank, DFI, digital bank, EMI, PSO and PSP
- ✓ Live dashboards by instrument and by category
- ✓ PDF and CSV reports for the board and auditors
- ✓ Assessment scope, notes and evidence on every requirement
- ✓ Owner / editor / viewer roles and a full audit trail
- ✓ White-label reports: your logo, header and footer on every page
- ✓ Email support

WHAT IT IS NOT

KSBPRC is a tracking and organisation tool. It does not give legal or audit advice, and using it does not make you compliant with, or certified against, anything. It is an independent product and is not affiliated with, endorsed by or approved by the State Bank of Pakistan; the official texts on sbp.org.pk always prevail.

© 2026 KIM

ARCHITECTURE

How a multi-tenant SaaS keeps tenants apart.

Client — any modern browser; HTTPS / TLS only, HSTS, strict security headers.

↓

Edge & app — Vercel. Next.js App Router. Middleware refreshes the session, enforces the two-factor step-up and the 30-minute idle timeout, and gates every workspace route. Server actions re-check role and membership on every write.

↓

Auth — Supabase. Hashed passwords (never seen by us), signed http-only session cookies, TOTP two-factor with a required step-up at sign-in.

Postgres with Row-Level Security. Every tenant table carries an organisation id; policies let members read and permitted roles write. The 1,504 requirements are shared, read-only reference data.

Storage — Supabase. A private bucket; each object's path starts with the workspace id and is governed by the same policies. Downloads only through a 60-second signed URL.

Off to the side — Lemon Squeezy. Merchant of Record. Cards are entered on Lemon Squeezy; we receive only a subscription record over a signed webhook. No card data on our servers.

WHY ONE TENANT CAN'T SEE ANOTHER

- ✓ **The fence is in the database.** A query runs as the signed-in user and the database filters every row by organisation; an application bug can't widen access.
- ✓ **Files inherit the fence.** Workspace A can't list, open or guess a file in workspace B.
- ✓ **Least privilege.** Owner, editor and viewer per workspace; seat and billing limits are database rules, not just hidden buttons.
- ✓ **Backed up and recoverable.** Managed Postgres and storage with daily backups and point-in-time recovery on the production tier.

© 2026 KIM

SIGN-IN, EVIDENCE AND CHANGE HISTORY

Signed in securely. Ready for the auditor.

- ✓ **Account security.** Two-factor authentication with any authenticator app, a 30-minute idle timeout, and a 12-character password policy with reuse history and lock-out after repeated failures.
- ✓ **Encryption and evidence.** TLS in transit, encrypted at rest. Evidence sits in a private store; every download is a fresh 60-second signed link, never a public URL.
- ✓ **Audit trail.** Every status change is recorded: who changed what, from what value, and when.
- ✓ **White-label reports.** Your organisation's logo, header title and footer line on every page. A consultancy hands each client a report in that client's own livery.
- ✓ **No lock-in.** Your assessment data leaves in open formats (PDF, CSV, evidence ZIP) whenever you want it.
- ✓ **Payments.** Card and PayPal through a Merchant of Record; global VAT and sales tax handled; no card data on our servers.

$500 per seat / year

5-day free trial, no card needed. No minimum — buy a single seat. Add or remove seats one at a time, pro-rated to your renewal date; seats are reassignable within the term at no extra cost. Cancel from the Billing page; access runs to the end of the paid year.

Start the free trial — kimsbp.app

Kim · kim_abdalian@yahoo.com · +973-3671-9993

Independent product of Kim. Not affiliated with, endorsed by or approved by the State Bank of Pakistan. Requirements are drawn from SBP's published circulars and cite them; the official texts on sbp.org.pk always prevail. SBP instruments and framework names are the property of their respective owners.

© 2026 KIM. ALL RIGHTS RESERVED.