IT Security Audit Report

Pakistan Financial Services Corp — Comprehensive Assessment | May 2026

EXECUTIVE SUMMARY

This security audit was conducted across Pakistan Financial Services Corp's Lahore and Karachi data centers. The assessment covered network infrastructure, access controls, data protection, and compliance with PDPB 2023 requirements. A total of 14 findings were identified: 4 critical, 5 high, 3 medium, and 2 low severity.

Severity	Count	Status
Critical	4	Open — Remediation Required
High	5	Open — Remediation Planned
Medium	3	In Progress
Low	2	Accepted Risk
TOTAL	**14**	**—**

COMPLIANCE OVERVIEW

Framework	Score	Gap Count
PDPB 2023	62%	8 gaps
ISO 27001	71%	5 gaps
PCI-DSS v4.0	58%	11 gaps
SBP Cyber Risk Framework	65%	7 gaps

DETAILED FINDINGS

ID	Finding	Severity	Status
SA-001	Unencrypted data at rest in Karachi DC	Critical	Open
SA-002	Default credentials on 12 network devices	Critical	Open
SA-003	No MFA for admin access to core switches	Critical	Open
SA-004	Unpatched VPN gateway (CVE-2026-XXXX)	Critical	Open
SA-005	Shared service accounts across Lahore DC	High	Planned
SA-006	No centralized log aggregation	High	Planned
SA-007	Expired SSL certificates on 3 portals	High	Planned
SA-008	Insufficient DDoS protection for SLIC portal	High	Planned
SA-009	Missing network segmentation for PCI zone	High	Planned
SA-010	Password policy < 12 char minimum	Medium	In Progress
SA-011	No automated vulnerability scanning	Medium	In Progress
SA-012	Backup encryption not verified	Medium	In Progress
SA-013	Vendor access review overdue	Low	Accepted
SA-014	Missing asset inventory for IoT devices	Low	Accepted

REMEDIATION ROADMAP

Priority	Action	Owner	Target
P1 — Immediate	Rotate all default credentials	Network Team	Week 1
P1 — Immediate	Patch VPN gateway (CVE-2026-XXXX)	Security Team	Week 1
P1 — Immediate	Enable MFA on all admin interfaces	IAM Team	Week 2
P1 — Immediate	Deploy encryption at rest (Karachi DC)	Infra Team	Week 3
P2 — Short-term	Centralize log aggregation (SIEM)	Security Team	Week 4
P2 — Short-term	Renew expired SSL certificates	Web Team	Week 2
P2 — Short-term	Segment PCI zone from general network	Network Team	Week 6
P2 — Short-term	Deploy DDoS protection for SLIC portal	Infra Team	Week 4
P2 — Short-term	Eliminate shared service accounts	IAM Team	Week 4
P3 — Medium-term	Implement 12+ char password policy	IAM Team	Week 8
P3 — Medium-term	Deploy automated vuln scanner	Security Team	Week 8
P3 — Medium-term	Verify backup encryption integrity	Infra Team	Week 6

CONCLUSION

Pakistan Financial Services Corp requires immediate attention to 4 critical findings that pose significant risk to data integrity and business continuity. Estimated remediation timeline for all critical items: 3 weeks. Full compliance with PDPB 2023 achievable within 12 weeks with dedicated resources.