EXECUTIVE WHITE PAPER

PAKISTAN'S NEW COMPLIANCE STACK

A CISO Advisory Perspective for Financial Institutions

Cyber Shield, PISF 2026, PVARA, and Pakistan's Emerging Data Governance Regime, Viewed Through GCC Regulatory Practice

TARGET AUDIENCE: EXECUTIVE AND SENIOR MANAGEMENT

Kim | CISO

CyAN Member | Cybersecurity Advisors Network

linkedin.com/in/kimabdalian

August 2026

Sources: SBP, National CERT, PVARA, Pakistan Digital Authority — Independent Regulatory Analysis

Table of Contents

Executive Summary

Advising financial institutions in Pakistan through 2025 and 2026 has meant tracking five regulatory developments moving at once, not one:

1. **Cyber Shield.** The State Bank of Pakistan's cyber resilience strategy is resetting cybersecurity governance for banks and payment institutions through 2030 [1][3].
2. **PISF 2026.** National CERT's Pakistan Information Security Framework, approved by the federal cabinet in August 2026, sets a horizontal national baseline for governance, risk, and incident response across all Critical Information Infrastructure, banking included [18][19].
3. **PVARA.** The Pakistan Virtual Assets Regulatory Authority, created by ordinance in July 2025 and made permanent through the Virtual Assets Act 2026, has opened a licensing regime for virtual asset service providers relevant to any bank exploring digital asset rails [4][5][6].
4. **PDA.** The Pakistan Digital Authority, established under the Digital Nation Pakistan Act, 2025, is building the national digital infrastructure, data-sharing, and AI governance backbone that every regulated entity will eventually plug into [8].
5. **Data Protection.** Pakistan's data protection landscape, still governed by the Prevention of Electronic Crimes Act (PECA) 2016 and its January 2025 amendment rather than a dedicated data protection statute, remains the least mature of the five, even as a Personal Data Protection Bill continues to move through the legislative process [9][10][11].

For a CISO who spent most of a 28-year career inside GCC Central Bank-regulated institutions, largely under the Central Bank of Bahrain, before shifting focus toward advising Pakistani financial institutions directly, the pattern is familiar: the GCC went through a similar layering exercise roughly a decade earlier, a national cybersecurity baseline first, a virtual asset regime second, a digital and AI governance layer third, and data protection legislation last. What is different in Pakistan is the compression: all five layers are landing inside roughly nineteen months, from the Digital Nation Pakistan Act in January 2025 to PISF 2026's cabinet approval in August 2026, leaving boards and CISOs little runway to respond.

This paper summarizes each of the five regimes, compares them to CBB, SAMA, and CBUAE practice, and closes with an advisory checklist. Stated plainly for boards: no single committee meeting can absorb five regulatory briefings. The answer is one integrated program with one owner, one roadmap, and one evidence base mapped to all five regulators, not five separate initiatives competing for the same budget and people.

1. The View From an Advisory Seat

Most of the technical control language here will not surprise a CISO who has operated under the CBB, SAMA, or CBUAE. Zero trust, board-level accountability, licensed custody of digital assets, and data localization are not novel; they are vocabulary GCC institutions have used for years. What is genuinely useful about advising inside Pakistan right now is the sequencing problem: five regulators, each moving at their own pace, converging on the same entities within the same budget cycle.

A Pakistani bank's CISO today needs a resilience roadmap aligned to Cyber Shield, a control set mapped to PISF 2026, a position on PVARA-licensed virtual asset activity, a plan for the PDA's data infrastructure, and a data protection posture built on PECA with a path to the PDP Act. The rest of this paper works through each pillar, then sequences the response using two decades of GCC practice.

2. Pillar One: SBP's Cyber Shield Resilience Strategy

Cyber Shield, announced by SBP on 16 February 2026, is described by the regulator as a roadmap to strengthen cyber resilience across the banking and payments sector through improved governance, expanded information-sharing, dedicated cyber talent development, and updated security practices [1][3]. Rather than a single circular, it functions as a multi-year strategy with phased milestones extending to 2030, and it requires every regulated bank, microfinance bank, development finance institution, electronic money institution, and payment system operator to formally align its internal cybersecurity program to the strategy's expectations [3].

Pakistan's national cyber coordination body, PKCERT, has reported 927 cyberattacks against Pakistani organizations across 2024 and 2025 combined, with a further 253 recorded in the first months of 2026, a trend its leadership has described as growing but so far contained [2]. That backdrop is reflected in two concrete developments since the strategy's launch. The Pakistan Banks' Association and SBP jointly ran the country's first industry-wide cyber drill between 12 and 19 January 2026, exercising 34 banks, microfinance banks, and payment institutions against a coordinated attack scenario [3]. Weeks later, Finance Minister Muhammad Aurangzeb convened bank chief executives and CISOs specifically to discuss AI-enabled attacks against digital banking channels, framing AI-driven fraud and social engineering as a board-level risk rather than a purely technical one [3]. Pakistan's admission to the Asia Pacific CERT community and to FIRST (the Forum of Incident Response and Security Teams, the principal global association coordinating incident response across national and sectoral CERTs) during 2026 further signals an intent to plug the country's incident-response capability into international information-sharing channels [2].

In advisory terms, the structure is consistent with how mature financial regulators sequence resilience mandates: near-term milestones emphasize governance, asset visibility, and incident-reporting discipline, while later phases push into more demanding technical and assurance requirements. Clients who treat Cyber Shield as a single compliance event rather than a five-year capability build are the ones most likely to face expensive rework in later phases.

Cloud Adoption and the Zero Trust Mandate

SBP officials speaking publicly in mid-2026 confirmed that Pakistani banks are increasingly adopting hybrid cloud infrastructure to support artificial intelligence workloads, since building AI infrastructure entirely on-premises requires capital most institutions cannot justify [2]. The regulator's expectation, articulated alongside that trend, is explicit: banks integrating public and private cloud must implement zero trust architecture, centralized identity and access management, cloud-native security monitoring integrated with on-premises systems, and consistent security policy enforcement across both environments [2]. This is the same control set GCC CISOs have been building toward under CBB, SAMA, and CBUAE cloud and outsourcing

expectations, and it maps cleanly onto globally recognized catalogs such as NIST CSF 2.0 [12] and ISO/IEC 27001:2022 [13], particularly the Annex A controls covering supplier relationships and information security for cloud services. This makes it one of the more straightforward pillars to advise on: the target architecture is already well understood, even if the timeline to get there is compressed.

An Illustrative Phasing Model

SBP has not published a detailed year-by-year milestone schedule for Cyber Shield in public materials; the regulator has described the strategy as phased through 2030 without itemizing each phase [1][3]. In the absence of that published detail, the table below sets out an illustrative three-horizon structure, built from how comparable multi-year resilience mandates, including SAMA's Cybersecurity Framework rollout, have typically sequenced in practice. Institutions should treat it as a planning scaffold to validate against SBP's own circulars as they are issued, not as a substitute for them.

Horizon	Typical Window	Characteristic Focus
Foundation	Years 1–2 (2026–2027)	Governance sign-off, asset and vendor inventories, incident classification and reporting discipline, sector-wide drill participation
Technical Uplift	Years 2–4 (2027–2029)	Zero trust and cloud-native architecture, identity-centric controls, AI and fraud-detection tooling, third-party risk assurance
Assurance & Maturity	Years 4–5 (2029–2030)	Independent testing, resilience validation, continuous CERT and FIRST information-sharing, board-level maturity reporting

Table A. Illustrative Cyber Shield phasing, based on comparable multi-year regulatory rollouts. SBP has not published itemized annual milestones; treat as a planning reference pending official circulars.

SBP Supervisory Expectations During Inspections

Drawing on how SBP and comparable GCC central banks conduct on-site and thematic reviews, Cyber Shield inspections are likely to test evidence rather than policy documents alone: named board or committee accountability that can answer direct questions, incident tickets that trace to the classification scheme in the institution's own policy, vendor risk assessments dated and refreshed rather than produced for the inspection, and proof of participation in sector exercises such as the January 2026 drill. Institutions that keep a live, dated evidence file mapped to Cyber Shield's expectations, rather than reconstructing one when an inspection is announced, consistently fare better in this kind of review.

3. Pillar Two: PISF 2026, the National Baseline

While SBP has been building a sector-specific cybersecurity mandate for banking, National CERT (PKCERT) has been building the national one. The Pakistan Information Security Framework (PISF 2026) was developed under the CERT Rules 2023, and National CERT submitted it to the federal cabinet in July 2026 after completing consultations with federal and provincial governments, regulators, and critical infrastructure operators [19]. The federal cabinet approved PISF 2026 in August 2026, describing it as an important guiding document for

the country's cybersecurity landscape and directing relevant authorities to ensure its implementation within the prescribed timeframe [18].

PISF 2026 is designed to establish a comprehensive, standardized system of information security requirements and to introduce uniform baseline standards with centralized oversight of cybersecurity matters [18]. Under the framework, in-scope organizations are required to establish formal cybersecurity governance structures, conduct regular risk assessments, implement standardized incident response procedures, maintain business continuity and disaster recovery plans, classify critical assets, protect personal data, conduct resilience testing, maintain coordination with sectoral and national CERTs, and provide regular cybersecurity awareness training to employees [19][20]. Implementation guidance built around the framework describes roughly thirteen mandatory compliance documents spanning information security, risk assessment, asset management, access control, incident response, and business continuity policy [20].

Scope is the detail that matters most for a financial institution. PISF 2026 is aimed at government bodies, regulatory authorities, and organizations designated as Critical Information Infrastructure (CII), a category that squarely includes SBP, the banking sector, and other regulated financial entities alongside SECP, NEPRA, OGRA, and the Higher Education Commission [21]. That means a Pakistani bank's CISO is not choosing between Cyber Shield and PISF 2026; both apply, and they need to be read together rather than in isolation.

Reading PISF 2026 Alongside Cyber Shield

The two frameworks are not redundant, but they do overlap, and the overlap is where an advisory function earns its keep. Cyber Shield is SBP's sector-specific resilience strategy, phased through 2030, with milestones tailored to banking, payments, and digital-banking-channel risk. PISF 2026 is the horizontal, cross-sector baseline, setting the governance, risk assessment, incident response, and documentation floor that applies to any CII entity regardless of sector. In practice this means a bank's governance structure, risk register, and incident response plan need to satisfy both a national auditor working from the roughly thirteen PISF 2026 documents and a banking supervisor working from Cyber Shield's milestones. Institutions that build a single control set mapped to both frameworks from the outset will avoid maintaining two parallel compliance programs that increasingly ask for the same evidence in different formats. This is the same lesson GCC institutions learned when NCA's Essential Cybersecurity Controls in Saudi Arabia arrived alongside SAMA's own Cybersecurity Framework: a national baseline and a sector-specific mandate coexisting is normal, but only if someone maps them to each other early.

The practical way to avoid dual compliance overhead is a single control-to-requirement matrix: one row per control, with columns showing which Cyber Shield milestone and which PISF 2026 document it satisfies. Built once, that matrix turns two audits into one evidence-gathering exercise rather than two, and it is the single highest-leverage artifact a Pakistani bank's GRC function can produce in 2026.

4. Pillar Three: PVARA and the Virtual Assets Act, 2026

The Pakistan Virtual Assets Regulatory Authority was established as an autonomous federal body under the Virtual Assets Ordinance, 2025, signed on 8 July 2025, and reports to the Ministry of Finance under Chairman Bilal Bin Saqib [4]. The Senate passed the Virtual Assets Bill on 28 February 2026 to give the authority

permanent legal cover before the original ordinance lapsed [6], and Pakistan's parliament subsequently passed the Virtual Assets Act, 2026, converting PVARA into a permanent statutory regulator with full power to license, supervise, suspend, and revoke virtual asset service providers, including exchanges, custodians, and token issuers [5].

The Act carries meaningful teeth. Operating without a license attracts penalties of up to PKR 50 million and up to five years' imprisonment, while unauthorized promotional activity for virtual assets carries a separate penalty of up to PKR 25 million and three years' imprisonment [5]. Existing operators were given a defined window to apply for a PVARA license or cease operations, licensing runs as a two-stage process beginning with a No-Objection Certificate before incorporation and followed by a full license, and the Act has extraterritorial reach, meaning foreign platforms serving Pakistani users may fall within scope [17]. PVARA has also been given the power to designate special virtual asset zones intended to attract blockchain companies, and it requires firms seeking a license to already hold recognition in a major jurisdiction such as the United States, the European Union, or Singapore, alongside compliance with Sharia principles under a dedicated scholars' committee [5]. HTX became one of the first exchanges to receive a No-Objection Certificate in December 2025 [5].

For banks, the immediately relevant detail is PVARA's own description of its coordination with the banking regulator: the authority has stated that banking rails for licensed virtual asset activity are being developed in coordination with the State Bank of Pakistan [7]. That is the point at which this pillar stops being a fintech story and becomes a CISO and compliance story. Any Pakistani bank asked to provide settlement, custody-adjacent, or on-ramp banking services to a PVARA-licensed VASP needs a control framework for that relationship well before the first account opens, covering AML/CFT alignment with FATF standards, wallet and key-management assurance from the counterparty, and a clear internal position on which categories of virtual asset activity the institution is willing to bank at all.

A GCC Comparison Point

The build-out sequence, presidential ordinance for speed, followed by full legislation, followed by a licensing regime with defined penalties and a transition window, mirrors how Bahrain and the UAE approached virtual asset regulation before PVARA existed. The Central Bank of Bahrain's Crypto-Asset Module and the Central Bank of the UAE's Virtual Assets Regulation of 2023 both took a similar path from sandbox-era guidance to a full licensing module [15][16]. The practical lesson for Pakistani institutions is that the licensing bar tends to rise, not fall, once the regime matures from ordinance to permanent statute, so early engagement with PVARA is worth more than waiting for the framework to fully settle.

VASP Risk Tiering Table

Not every PVARA-licensed relationship carries the same risk to a bank, and treating them all identically either overblocks legitimate business or underprotects the institution. The table below adapts a three-tier categorization from how GCC banks tier crypto-adjacent counterparties under CBB and CBUAE guidance.

Tier	Relationship Type	Primary Risk	Due Diligence Depth
Tier 1 — Highest	Settlement and fiat on/off-ramp relationships	AML/CFT exposure and reputational risk	Full board-level review; ongoing enhanced monitoring
Tier 2 — Elevated	Custody-adjacent and wallet infrastructure relationships	Key-management and smart-contract technical risk	Specialist technical review, not standard vendor assessment
Tier 3 — Standard	Payment-rail or API connectivity relationships	Indirect exposure via counterparty's client base	Standard vendor due diligence with periodic monitoring

Table D. VASP relationship risk tiering, adapted from GCC crypto-counterparty risk practice.

A VASP Onboarding Control Framework

- Confirm current PVARA licensing status directly, not through the counterparty's own representation, and re-verify at each renewal cycle.
- Require evidence of AML/CFT program alignment with FATF standards, including Travel Rule compliance for cross-border virtual asset transfers.
- Commission independent technical assurance over wallet architecture and key-management controls before onboarding, not as a post-incident exercise.
- Define, in writing and at board level, which categories of virtual asset activity the institution will and will not bank, so front-office teams are not making that call deal by deal.
- Set enhanced, time-bound monitoring thresholds for the relationship's first several months rather than defaulting to standard periodic review cycles.

5. Pillar Four: The Pakistan Digital Authority and the Digital Nation Pakistan Act, 2025

The Pakistan Digital Authority was established under the Digital Nation Pakistan Act, 2025, enacted on 29 January 2025 with immediate effect, as a statutory corporate body tasked with accelerating digital transformation across government and the economy [8]. Under Section 8 of the Act, the PDA develops and maintains the National Digital Masterplan, issues and enforces regulations, guidelines, and standards to support it, and is explicitly mandated to establish frameworks for data protection, privacy, and responsible data governance across Pakistan [8].

Three elements of the PDA's mandate are directly relevant to a financial institution's CISO and IT security function. First, the Authority is building secure digital infrastructure intended to let public institutions share data through governed, auditable pathways, which will eventually intersect with how banks exchange data with government systems for KYC, tax, and identity verification purposes. Second, the PDA maintains an official register of standards for what it describes as sovereign digital infrastructure, a reference point that regulated entities should expect to be pulled into procurement and architecture decisions over time. Third, the Authority has published a set of national AI principles framed around AI that serves public value and

remains under human accountability, a nine-principle statement of direction rather than a binding technical standard for now, but one that signals where AI governance obligations are likely to land [8].

From an advisory standpoint, the PDA is the least immediately actionable of the five pillars for a bank today, but it is the one most likely to reshape the operating environment over a five-year horizon, since it sits above sector regulators as the architect of Pakistan's national digital and data infrastructure. Institutions that treat it as background noise now risk having to retrofit their data architecture and AI governance model once PDA standards mature into binding requirements.

Expected Timeline and Banking Architecture Impact

The PDA has not published a binding compliance deadline for financial institutions, and its National Digital Masterplan, sovereign infrastructure standards register, and AI principles remain, as of August 2026, primarily directional rather than enforced [8]. Based on how comparable national digital authorities in the GCC have matured, most notably the UAE's federal digital government program, the realistic sequence is standards publication and voluntary alignment first, integration requirements for government-facing data exchange second, and binding sector-specific enforcement, likely routed through SBP rather than the PDA directly, last. For a bank's architecture team, the practical implication is that new KYC, tax, and identity-verification integrations built today should be designed against the PDA's published interoperability and sovereign infrastructure standards where they exist, since retrofitting a live integration is materially more expensive than building to the standard the first time.

AI Governance Obligations on the Horizon

The PDA's nine AI principles, framed around AI that serves public value and remains under human accountability, are a statement of direction rather than a technical control set, but they signal the same trajectory GCC institutions have already navigated through the EU AI Act and ISO/IEC 42001. A Pakistani bank already running AI-driven fraud detection or credit decisioning should expect, over time, to need a documented AI risk classification, human-in-the-loop controls for high-impact decisions, and model governance evidence broadly consistent with ISO/IEC 42001, positioning institutions that have already built AI governance for other jurisdictions to extend that same program to Pakistan rather than starting over.

The table below sets out a minimum AI governance control set a Pakistani financial institution can reasonably build toward now, ahead of binding PDA technical standards, mapped to the global references institutions with GCC or EU AI Act exposure already use.

Control Area	Minimum Control	Reference
Risk Classification	Every AI use case classified by impact before deployment, not after	ISO/IEC 42001:2023; EU AI Act
Human Oversight	Human-in-the-loop review for high-impact decisions (credit, fraud blocking)	PDA's nine AI principles; EU AI Act Art. 14
Model Governance	Documented model inventory, validation records, and change control	ISO/IEC 42001:2023 Clause 8

Control Area	Minimum Control	Reference
Data Governance for AI	Training and inference data mapped to data classification and localization rules	Draft PDP Bill; PDA sovereign infrastructure standards
Vendor AI Assurance	Third-party AI tools assessed for explainability and bias before procurement	ISO/IEC 42001:2023; NIST AI RMF

Table E. Minimum AI governance controls for Pakistani financial institutions, mapped to global references.

6. Pillar Five: Data Protection, Still the Least Mature Layer

Pakistan has not yet enacted a dedicated, comprehensive data protection law. The Personal Data Protection Bill, 2025 remains in draft form, and in its place PECA 2016 continues to serve as the primary statutory tool addressing misuse of personal information, penalizing unauthorized access, unauthorized copying, and system interference [9][10]. A significant amendment, the Prevention of Electronic Crimes (Amendment) Act, 2025, took effect in January 2025 and transferred exclusive cybercrime investigation authority from the Federal Investigation Agency's Cyber Crime Wing to a newly created National Cyber Crime Investigation Agency (NCCIA), meaning PECA complaints for unauthorized data disclosure must now be directed to the NCCIA [9]. The same period saw the creation of a Social Media Protection and Regulatory Authority (SMPRA) with powers to monitor and require removal of unlawful or offensive content, and the introduction of data localization requirements for telecom operators under CTDISR-2025 [9].

The draft Personal Data Protection Bill, once enacted, would introduce more familiar data protection concepts: a defined data subject and data controller relationship, consent-based lawful processing, rights of erasure and withdrawal of consent, and rules on cross-border data transfer that would only permit transfers to jurisdictions offering equivalent protection, with critical personal data required to remain on servers located inside Pakistan [11]. Commentary on the draft has also raised concerns that it grants extensive exemptions to state agencies while imposing full compliance obligations on private businesses, and that its scope reaches any organization processing the personal data of individuals in Pakistan regardless of where that organization is physically located, an extraterritorial design similar to the GDPR and to Bahrain's own PDPL [22].

For a Pakistani financial institution, the practical posture today is to comply with PECA and its 2025 amendment as a floor, while building a data governance program to the standard the pending PDP Bill is likely to require, since SBP already expects banks to maintain data protection frameworks in the financial sector as part of ordinary supervisory practice, and retrofitting a control environment after a comprehensive law is enacted is materially more expensive than building toward it in advance [9].

PECA Today Versus the Draft PDP Bill

The table below lines up what PECA and its 2025 amendment already require against what the draft Personal Data Protection Bill is expected to add, based on its publicly available provisions [9][10][11].

Dimension	PECA 2016 + 2025 Amendment (Current)	Draft PDP Bill (Expected)
Legal Character	Criminal statute; penalizes unauthorized access, copying, and system interference	Dedicated civil data protection framework with a regulatory Commission
Individual Rights	Not rights-based; complaint and investigation driven via the NCCIA	Consent, withdrawal, erasure, and objection rights for data subjects
Cross-Border Transfer	No general transfer regime; CTDISR-2025 localization applies to telecom data only	Transfers restricted to jurisdictions with equivalent protection; critical data localized
State Agency Scope	Investigative powers centralized in the NCCIA	Broad exemptions for state agencies flagged as a concern by civil society commentary
Extraterritorial Reach	Limited to acts and systems within Pakistan's jurisdiction	Applies to any entity processing Pakistani residents' data, regardless of location

Table B. PECA's current data-related obligations compared with the draft Personal Data Protection Bill's known provisions.

Data Localization Implications for Banks

The localization signal is already present in two places even before the PDP Bill is enacted: CTDISR-2025 requires data localization for telecom operators, and the PDP Bill's draft text would require critical personal data to remain on servers located inside Pakistan [9][11]. Banks running core banking, fraud analytics, or AI model training on cloud infrastructure outside Pakistan should treat this as a live architecture question now, not a future compliance item, since migrating a production data estate after a localization requirement takes effect is a materially larger project than designing for it from the outset. The practical hedge is to classify data now against the categories the PDP Bill is likely to treat as critical, so the institution knows in advance which workloads would need to move.

Lessons From Bahrain's PDPL Rollout

Bahrain enacted its own Personal Data Protection Law well before most of its GCC peers, and the experience of bringing a Central Bank-regulated institution into compliance with it offers a directly transferable lesson: the hardest part is rarely the legal text itself, it is the data inventory and lawful-basis mapping exercise that has to happen before any policy can be written. Pakistani financial institutions that start that inventory now, against PECA's existing requirements and the draft PDP Bill's likely shape, will be materially better positioned than those that wait for the Bill's final text before starting.

7. Regulatory Intersections and GCC Benchmarks

Five separate regulators rarely announce how their mandates intersect; that mapping is left to the institutions they regulate. The figure below shows the shape of the problem: five distinct tracks, moving on five different timelines, converging on the same board and the same CISO.

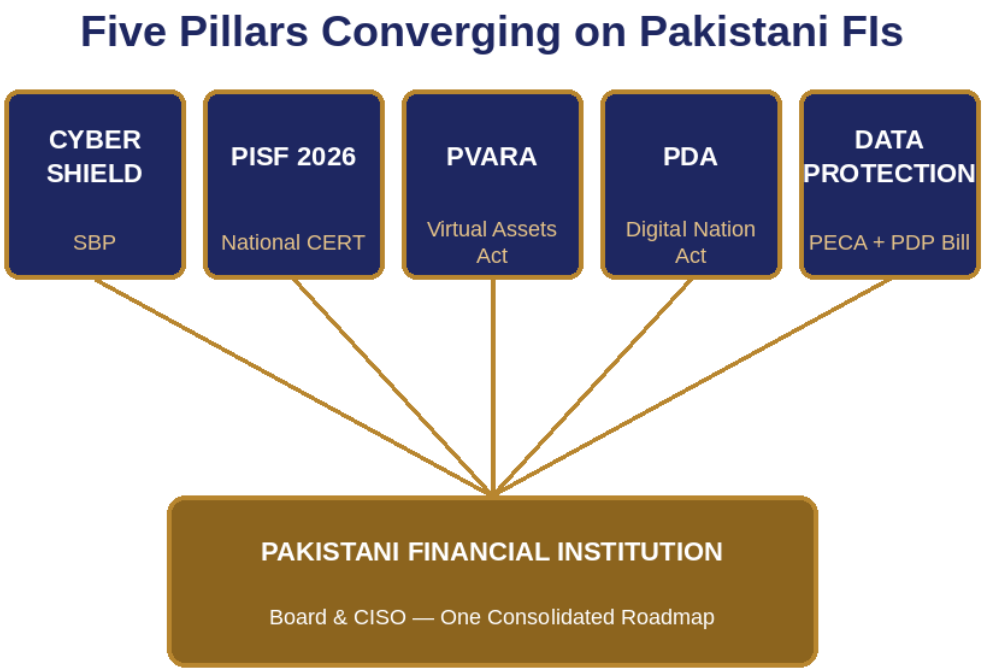

Figure 1. Five regulatory pillars converging on a single regulated entity.

The clearest example of that convergence is Cyber Shield and PISF 2026, which share a substantial governance, risk, and incident-response core even though one is banking-specific and the other is a national baseline.

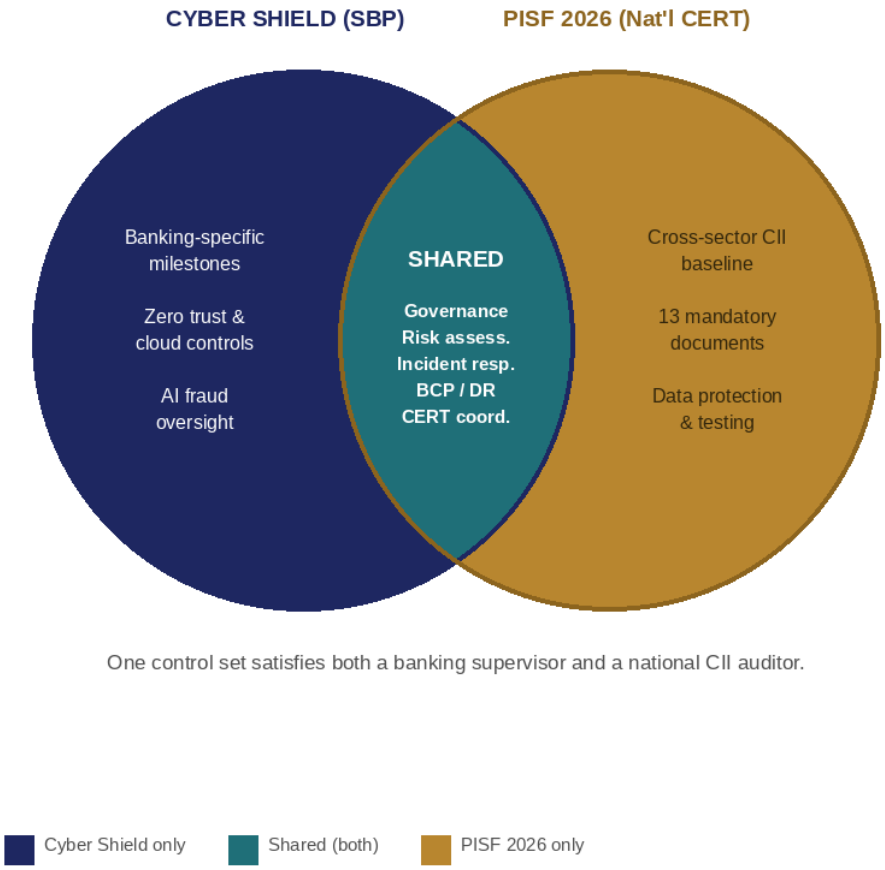

Figure 2. Overlap between SBP's Cyber Shield and National CERT's PISF 2026.

Sequencing matters as much as content. The timeline below places all five developments on a single axis, from the Digital Nation Pakistan Act in January 2025 through PISF 2026's cabinet approval in August 2026.

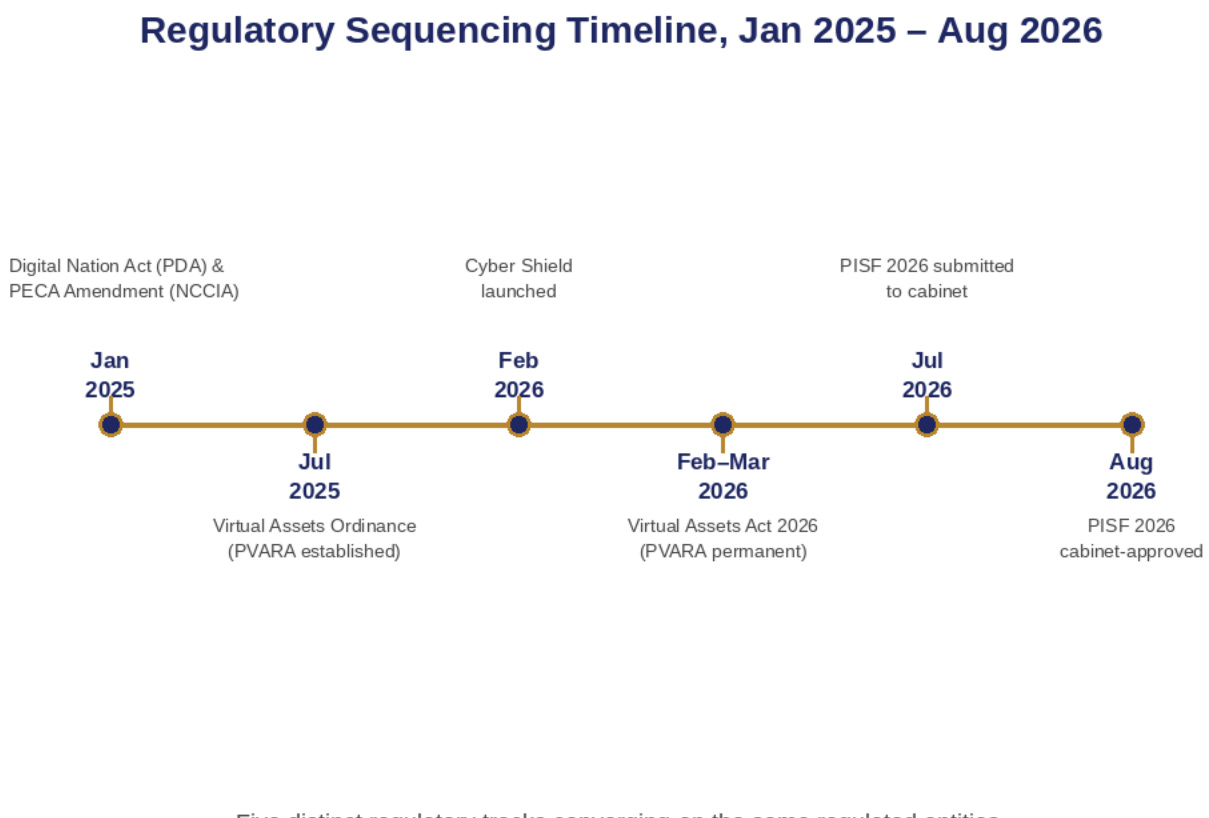

Figure 3. Regulatory sequencing timeline, January 2025 to August 2026.

The table below summarizes how each of Pakistan's five 2025-2026 regulatory pillars maps to the frameworks and regulators a GCC-experienced CISO would already recognize.

Pillar	Pakistan 2025-2026 Requirement	GCC / Global Reference
Governance & Oversight	Board-level alignment with Cyber Shield milestones; formal cyber program sign-off	NIST CSF 2.0 GOVERN; ISO/IEC 27001:2022 Clause 5
Cloud & Third-Party Risk	Zero trust architecture; centralized IAM; cloud-native monitoring	NIST SP 800-53 SR family; ISO/IEC 27001 A.5.19-A.5.23
Payment Card Security	Continued PCI DSS certification across the payments ecosystem	PCI DSS v4.0.1
Incident Response & Coordination	Sector-wide drills; CERT and FIRST membership; escalation to regulator	NIST CSF 2.0 RESPOND/RECOVER; ISO/IEC 27001 A.5.24-A.5.28
National Baseline (PISF 2026)	13 mandatory documents; governance, risk, IR, BCP/DR, asset classification, CERT coordination [18][19][20]	NIST CSF 2.0; SA NCA Essential Cybersecurity Controls
Virtual Asset Licensing	PVARA NOC then full license; AML/CFT per FATF; PKR 50m / 5-year penalty for unlicensed activity [5]	Contrast: CBB Crypto-Asset Module; CBUAE Virtual Assets Regulation 2023

Pillar	Pakistan 2025-2026 Requirement	GCC / Global Reference
National Digital & AI Governance	PDA National Digital Masterplan; sovereign infrastructure standards; nine AI principles [8]	EU AI Act; ISO/IEC 42001:2023
Data Protection	PECA 2016 + 2025 amendment; NCCIA; draft Personal Data Protection Bill [9][11]	GDPR; Bahrain PDPL

Table 1. Mapping Pakistan's five-pillar 2025-2026 regulatory stack to frameworks and regulators commonly used across GCC-regulated institutions.

Where Pakistan's Stack Still Trails GCC Maturity

Mapping requirements to frameworks shows equivalence in intent; it does not show equivalence in maturity. The assessment below is the author's own advisory judgment, based on direct experience operating under both regimes, not an official finding by any regulator.

Dimension	Pakistan, August 2026	Mature GCC Equivalent
Regulatory Track Record	Under one year old for four of five pillars; supervisory practice still forming	CBB, SAMA, CBUAE frameworks tested through multiple inspection cycles
Published Detail	High-level strategies and principles; itemized technical standards still emerging	Detailed rulebooks with clause-level technical requirements
Cross-Regulator Coordination	Five regulators publishing independently; no published joint mapping yet	Established coordination between central bank and national cyber authority
Data Protection Legislation	No enacted comprehensive law; PECA serves as an interim substitute	Bahrain PDPL and equivalents enacted and enforced for several years

Table C. Advisory assessment of maturity gaps between Pakistan's emerging stack and established GCC frameworks.

8. Governance Expectations: What Boards Must Demonstrate

A phased, board-accountable strategy such as Cyber Shield shifts the question regulators ask from "do you have controls" to "can you demonstrate ownership and trajectory." Based on the pattern established by comparable frameworks, including the CBB's own cyber risk management expectations, boards of SBP-regulated entities should expect to demonstrate the following over the life of the strategy:

- Named accountability for the cyber program at board or board-committee level, not delegated implicitly to IT.
- A documented, tested incident response and business continuity plan with defined escalation thresholds and regulatory notification triggers.
- Evidence of participation in sector-wide exercises, such as the January 2026 PBA/SBP drill, rather than internal testing alone.

- A vendor and cloud risk register that reflects zero trust and identity-centric controls, not legacy perimeter assumptions.
- A credible narrative on AI-related risk, given the Finance Ministry's explicit focus on AI-driven threats to digital banking channels [3].
- A documented position on virtual-asset-adjacent banking relationships, given PVARA's stated coordination with SBP on banking rails [7].
- A mapped control set showing how the institution's Cyber Shield program also satisfies PISF 2026's roughly thirteen mandatory governance, risk, and incident response documents [19][20].

None of this is unfamiliar to a CISO who has reported into a GCC Central Bank-regulated board. The value of tracking Pakistan's rollout in an advisory capacity is in the sequencing: because all five pillars are phased over multi-year horizons, they offer a forward-looking template for how a regulator moves an entire sector from baseline compliance to demonstrable resilience, useful benchmarking for any GRC function building its own multi-year roadmap.

Board Dashboard Template

The table below is a ready-to-use starting template. Boards should populate the target and current-status columns quarterly rather than treating this as a one-time exercise.

KPI	Target	Frequency	Owner
Cyber Shield governance milestones with named, dated owners	100%	Quarterly	CISO
Open PISF 2026 documentation gaps (of ~13 mandatory items)	0 open	Quarterly	Head of GRC
Active PVARA-licensed VASP relationships with current AML/CFT review	100% current	Monthly	Head of Compliance
Critical data classified against draft PDP Bill localization categories	100%	Semi-annual	Chief Data Officer / CISO
Days since last sector-wide IR drill / board cyber tabletop	< 180 days	Ongoing	CISO
AI use cases with documented risk classification (Table E)	100%	Quarterly	Head of AI Governance / CISO

Table F. Board Dashboard Template for the five-pillar compliance program. Populate Target and status columns per institution.

9. Advisory Recommendations for Pakistani Financial Institutions

For CISOs and GRC Leaders Inside Pakistan

- Build a single consolidated roadmap that sequences Cyber Shield milestones, PISF 2026 documentation, PVARA-adjacent banking controls, PDA data-sharing readiness, and PECA-to-PDP-Bill data governance uplift together, rather than running five disconnected workstreams.

- Treat SBP's zero trust and centralized IAM expectations for hybrid cloud as the minimum architecture bar for any new AI or cloud initiative, since it is likely to be examined regardless of which pillar prompted the investment.
- Establish a formal control framework, covering AML/CFT, wallet assurance, and product approval, before agreeing to bank any PVARA-licensed virtual asset service provider.
- Start the data inventory and lawful-basis mapping exercise against PECA today, using the draft Personal Data Protection Bill's known provisions as the target state, rather than waiting for the Bill's final enactment.

For Boards Weighing GCC Benchmarks

- Use Cyber Shield's 2026-2030 phasing, PISF 2026's cabinet approval, and PVARA's ordinance-to-statute path as reference points when sequencing multi-year GRC investment, since all three mirror patterns the CBB, SAMA, and CBUAE have already run.
- Consider whether the institution's own sector-wide incident response testing matches the coordinated-drill model SBP and the Pakistan Banks' Association piloted in January 2026.
- Where AI-driven fraud and social engineering are on the board agenda, note that Pakistan's Finance Ministry has already elevated this from a technical to an executive-level discussion, a useful data point when framing AI risk for any board.

10. Appendix: The CISO Action Pack

The following is a starting scaffold, not a substitute for a tailored gap assessment. It is designed to be adapted to a specific institution's current maturity within the first working session after this paper is read.

180-Day Plan

- Weeks 1–4: Appoint a single accountable owner for the consolidated five-pillar roadmap and secure board or board-committee sponsorship.
- Weeks 4–9: Inventory current state against Cyber Shield, PISF 2026, and PECA requirements using existing policies, risk registers, and incident logs.
- Weeks 9–14: Build the Cyber Shield / PISF 2026 control-to-requirement matrix described in Pillar Two, identifying genuine gaps versus documentation gaps.
- Weeks 14–19: Classify any existing or planned PVARA-adjacent banking relationships against the three-tier risk categorization in Pillar Three.
- Weeks 19–23: Close first-wave technical gaps surfaced during the inventory, such as IAM cleanup, logging coverage, and initial zero trust milestones, ahead of the board review.
- Weeks 23–26: Present a board-level status report using the sample KPIs above, with a resourced plan for the remaining six months of the twelve-month roadmap.

12-Month Roadmap

- Months 1–6: Execute the 180-day plan above in full — governance foundation, named ownership, committee reporting lines, the Cyber Shield / PISF 2026 mapping matrix, VASP risk tiering, and first-wave technical gap closure.
- Months 7–9: Complete remaining technical uplift, zero trust architecture milestones, a fully operational VASP onboarding control framework, and data classification for localization readiness.
- Months 9–11: Run or participate in a sector-wide incident response exercise; complete the first full internal audit against the consolidated control matrix.
- Month 12: Board-level maturity review against all five pillars; refresh the roadmap for the following year based on any new circulars, regulations, or the PDP Bill's enactment status.

Control Mapping Checklist

- Governance: named owner, committee charter, board reporting cadence documented and current.
- Risk: enterprise risk register with the five pillars represented as distinct risk lines, each with a control owner, underpinned by a maintained Risk and Control Self-Assessment (RCSA) register that ties each control to its test evidence and reassessment date.
- Incident Response: classification scheme, escalation thresholds, and regulatory notification triggers mapped to both Cyber Shield and PISF 2026 requirements.
- Third-Party & VASP Risk: vendor and VASP due diligence records dated, current, and tiered by risk category.
- Data Governance: data inventory and lawful-basis mapping complete for at least critical and sensitive categories.
- Evidence: a single, live, dated evidence file an inspector or auditor could review without advance notice.

Conclusion

Pakistan's financial institutions are being asked to absorb five regulatory reforms in the space of about nineteen months: a sector-specific cybersecurity resilience strategy, a national information security baseline, a virtual asset licensing regime, a national digital and AI governance authority, and the early groundwork for comprehensive data protection law. None of these five pillars is individually unfamiliar to a CISO with GCC Central Bank experience, but the compression is real, and it is the compression, not the individual requirements, that makes an integrated advisory approach worth more than treating each regulator's mandate in isolation. Institutions that build one consolidated roadmap across Cyber Shield, PISF 2026, PVARA, the PDA, and Pakistan's evolving data protection regime now will be materially better positioned than those that respond to each mandate as it separately comes due.

Looking toward 2027 and beyond, the most likely next developments are enactment of the Personal Data Protection Bill, itemized technical milestones for Cyber Shield's later phases, PDA standards moving from directional to binding, and closer published coordination between SBP, National CERT, and PVARA as their

mandates continue to overlap in practice. Institutions that build the consolidated roadmap this paper describes now will be extending an existing program when each of those developments lands, rather than starting a new one.

About the Author

Kim | CISO

linkedin.com/in/kimabdalian

Kim is a Chief Information Security Officer and independent advisor on cybersecurity, AI governance, and IT security strategy to financial institutions in Pakistan and across the GCC, with more than 28 years of experience in information security leadership, risk management, and IT governance, including over 20 years within GCC Central Bank-regulated institutions. He has led enterprise security, risk, and compliance functions across Bahrain and the wider GCC and North Africa region, maintaining continuous PCI DSS certification with zero critical findings and directing regulatory engagement across Central Bank mandates including the CBB, SAMA, CBUAE, CBJ, and BDL. He now applies that regulatory depth to advising Pakistani financial institutions navigating SBP's Cyber Shield strategy, National CERT's PISF 2026 baseline, PVARA's virtual asset licensing regime, the Pakistan Digital Authority's national digital governance mandate, and the country's evolving data protection landscape, alongside continued work in AI governance and EU AI Act implementation, digital asset and stablecoin security, and cybersecurity GRC across the GCC.

Kim holds the CISM, CCSP, CDPO, and CBCMP certifications and is a Professional Engineer registered with the Pakistan Engineering Council. He is a Platinum Member of ISACA, a Member of the Pakistan Engineering Council (MPEC), a member of Cyberr®, and a Member of the Cybersecurity Advisors Network (CyAN).

References

[1] State Bank of Pakistan, "Cyber Shield – The Cyber Resilience Strategy for Regulated Entities," press release, Feb. 16, 2026. [Online]. Available: https://www.sbp.org.pk. [Accessed: Aug. 15, 2026].

[2] Business Recorder, "Cyber defence: Public, private entities told to set up 'SOCs' in 6 months," Jul. 2, 2026. [Online]. Available: https://www.brecorder.com/news/amp/40428085. [Accessed: Aug. 15, 2026].

[3] Let's Data Science, "Pakistan Strengthens Banking Cybersecurity with Cyber Shield Initiative," May 3, 2026. [Online]. Available: https://letsdatascience.com/news/pakistan-strengthens-banking-cybersecurity-with-cyber-shield-eb2ea3d4. [Accessed: Aug. 15, 2026].

[4] Wikipedia, "Pakistan Virtual Assets Regulatory Authority." [Online]. Available: https://en.wikipedia.org/wiki/Pakistan_Virtual_Assets_Regulatory_Authority. [Accessed: Aug. 15, 2026].

[5] The Block, "Pakistan parliament passes Virtual Assets Act formalizing crypto regulatory authority," Mar. 6, 2026. [Online]. Available: https://www.theblock.co/post/392665. [Accessed: Aug. 15, 2026].

[6] I. A. Khan, "Senate passes Virtual Assets Bill to formalise crypto regulator," Dawn, Feb. 28, 2026. [Online]. Available: https://www.dawn.com/news/1976346. [Accessed: Aug. 15, 2026].

[7] TradingView / Cointelegraph, "Pakistan's parliament passes the Virtual Assets Act of 2026," Mar. 6, 2026. [Online]. Available: https://www.tradingview.com/news/cointelegraph:95a02804a094b:0. [Accessed: Aug. 15, 2026].

[8] Wikipedia, "Pakistan Digital Authority." [Online]. Available: https://en.wikipedia.org/wiki/Pakistan_Digital_Authority. [Accessed: Aug. 15, 2026].

[9] Recording Law, "Pakistan Data Privacy Laws: PECA and Personal Data Protection Bill Guide (2026)," May 20, 2026. [Online]. Available: https://www.recordinglaw.com/world-laws/world-data-privacy-laws/pakistan-data-privacy-laws/. [Accessed: Aug. 15, 2026].

[10] DLA Piper, "Data protection laws in Pakistan," Data Protection Laws of the World. [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=law&c=PK. [Accessed: Aug. 15, 2026].

[11] International Bar Association, "Data privacy and protection in Pakistan." [Online]. Available: https://www.ibanet.org/data-privacy-and-protection-in-Pakistan. [Accessed: Aug. 15, 2026].

[12] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, Feb. 26, 2024. doi: 10.6028/NIST.CSWP.29.

[13] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022.

[14] PCI Security Standards Council, Payment Card Industry Data Security Standard, Version 4.0.1, 2024.

[15] Central Bank of Bahrain, Rulebook Volume 6: Crypto-Asset Module (CRA).

[16] Central Bank of the United Arab Emirates, Virtual Assets and Related Activities Regulation, 2023.

[17] ComplyFactor, "Pakistan Virtual Assets Act 2026: Complete Guide to PVARA Licensing and Compliance," Mar. 7, 2026. [Online]. Available: https://complyfactor.com/pakistan-virtual-assets-act-2026-complete-guide-to-pvara-licensing-and-compliance/. [Accessed: Aug. 15, 2026].

[18] TechJuice, "Federal Cabinet Approves Pakistan Information Security Framework 2026," Aug. 2026. [Online]. Available: https://www.techjuice.pk/federal-cabinet-approves-pakistan-information-security-framework-2026/. [Accessed: Aug. 15, 2026].

[19] ProPakistani, "Govt Prepares New Security System to Hunt Hackers And Avoid Online Disasters," Jul. 17, 2026. [Online]. Available: https://propakistani.pk/2026/07/17/govt-prepares-new-security-system-to-hunt-hackers-and-avoid-online-disasters/. [Accessed: Aug. 15, 2026].

[20] SecureWave Advisors, "Pakistan Information Security Framework (PISF)." [Online]. Available: https://securewaveadvisors.com/services/pakistan-information-security-framework-pisf/. [Accessed: Aug. 15, 2026].

[21] Business Recorder, "Pakistan govt entity hit by cyberattack last week, official says," Jul. 1, 2026. [Online]. Available: https://www.brecorder.com/news/40428063. [Accessed: Aug. 15, 2026].

[22] GenderIT.org, "Between Privacy and Power: The Fine Line in Pakistan's Data Protection Bill." [Online]. Available: https://www.genderit.org/articles/between-privacy-and-power-fine-line-pakistans-data-protection-bill. [Accessed: Aug. 15, 2026].

Disclaimer

This white paper is provided for general informational and educational purposes only and reflects the author's independent professional analysis of publicly available information. It does not constitute legal, regulatory, investment, or compliance advice, and should not be relied upon as a substitute for consultation with qualified legal, compliance, or risk advisors, or for direct engagement with the State Bank of Pakistan, National CERT, PVARA, the Pakistan Digital Authority, or any other relevant regulator. Regulatory requirements referenced herein, including Cyber Shield, PISF 2026, the Virtual Assets Act 2026, and the draft Personal Data Protection Bill, are evolving and subject to change; readers should verify current requirements directly with the issuing authority before taking any action. The views expressed are those of the author and do not necessarily represent the views of any current or former employer or organization.