CYBER SILO

PKCERT

PAKISTAN INFORMATION SECURITY FRAMEWORK (PISF) 2025

STRATEGIC SUMMARY & APPLICABILITY

2025

Published by: NCERT / PKCERT
Summarized by: CyberSilo | December 2025

EXECUTIVE SUMMARY

Released Date	November 2025
Framework Author	National Computer Emergency Response Team (nCERT) a.k.a PKCERT
Pre-Req Documents	National Cybersecurity Policy 2021 and CERT Rules 2023
Effective Date	Immediate upon release

Purpose, Applicability & Regulatory Cadence

Purpose:

Designed to fortify resilience across government and critical service infrastructures. The framework establishes mandatory security controls for:

Secure Operations | Risk Management | Incident Detection and Response

Applicability:

- Federal and Provincial Government Departments
- Autonomous Bodies
- Public Corporations
- National and Sectoral CERTs
- Designated Critical Information Infrastructures (CIIs)

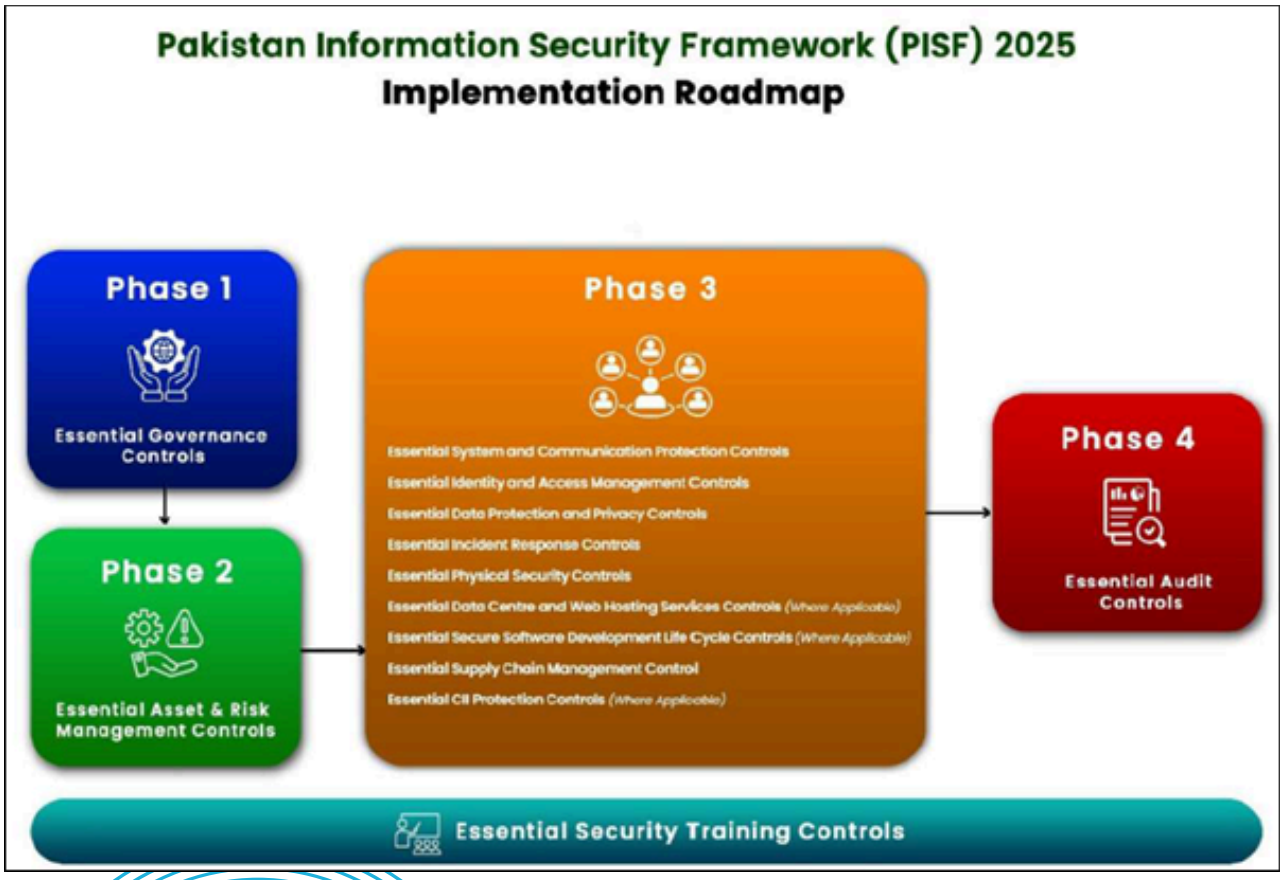
Regulatory Cadence:

Incident reporting to Sectoral CERT within 72 hours; Annual Internal & External Audits.

Phase and Control Mappings

Category	Description
1. Asset & Risk Mgmt.	• Classify Most Critical assets/services • Align controls proportionately with Confidentiality, Integrity, and Impact.
2. Continuous Improvement	• CSA adoption • IAM/Risk/Training KPIs • Remediation Tracking • Alignment with nCERT/NTISB guidance

3. Governance Controls	• Independent cybersecurity function led by CISO/CIIO • Steering Committee Oversight • RACI documentation • Top Management Responsible for Funding, Structure, And Accountability.
4. Asset Hygiene	• Maintain official Asset Register with Lifecycle Metadata • Secure Decommissioning; • Configuration Baselines • Logging retention ≥12 months for critical systems
5. SSDLC	• Security-by-Design • Code Reviews • SAST/DAST • SBOM Tracking • Penetration Testing • CI/CD Security Gates • Secrets Management
6. Supply Chain Security	• Vendor Due Diligence • Contractual Clauses (Confidentiality, Audit Rights, Breach Notice) • Pre-Procurement Validation • KPIs & Ongoing Audits
7. Supply Chain Security	• JML Processes with Timely Revocation • Least Privilege & Segregation of Duties • MFA for remote/admin • Privileged Access Vaulting, Monitoring & Periodic Recertification.
8. Incident Responses	• SOC/SIEM Monitoring • IR Playbooks and Forensics • RCA • Lessons Learned • CERT liaison • MTTD/MTTR metrics
9. Data Protection & Privacy	• PIAs • Retention Controls • Encryption in Transit/at Rest • Data Subject Rights Workflows. • Consent where required for Lawful Basis
10. Data Center & Physical Security	• Cabling SOPs • Visitor Logging • Auditable Trails • Environmental Controls • NGFW, WAF, IDS/IPS, DLP, DDoS
11. Training & Awareness	• Role-Based Training • Phishing Simulations • Mandatory Cybersecurity Awareness • Leadership Cyber-Risk Education



1) Essential System & Communication Protection Controls

Purpose: Secure organizational systems, networks, and communication channels with defense-in-depth.

Sr#	Sub-Point	Description
1.1	Baseline Hardening	Apply secure configurations for OS, network, and middleware; disable unused services and ports.
1.2	Secure Protocols	Use TLS/HTTPS/SSH; deprecate weak ciphers and legacy versions.
1.3	Network Segmentation	Implement VLANs/DMZs; isolate critical services and administrative networks.
1.4	Advanced Defenses	Deploy NGFW, WAF, IDS/IPS, anti-DDoS; tune controls with current threat intelligence.
1.5	Secure Email	Enforce SPF/DKIM/DMARC; use anti-phishing gateways with sandboxing.
1.6	Endpoint/Server Monitoring	Monitor via EDR/NDR; integrate alerts into SIEM/SOC for centralized visibility.
1.7	Data Encryption	Encrypt data in transit and at rest; manage cryptographic keys with separation of duties.
1.8	Least Privilege	Enforce least privilege access; routinely review privileged actions and admin sessions.
1.9	Centralized Logging	Centralize logs; retain critical logs ≥12 months; ensure time synchronization (NTP)
1.10	Patch Management	Patch based on risk; verify remediation with scans and change records.
1.11	Configuration Integrity	Validate configuration baselines; monitor for drift and maintain integrity.
1.12	Backup & Recovery	Test backup/restoration; document RTO/RPO; rehearse recovery procedures.
1.13	Evidence Retention	Maintain auditable evidence: configs, logs, test reports, approvals.

2) Essential Supply Chain Controls

Purpose: Manage third-party risks across procurement, delivery, operation, and offboarding.

Sr#	Sub-Point	Description
2.1	Vendor Due Diligence	Perform due diligence on vendors; assess certifications, security posture, and past incidents.
2.2	Security Clauses	Include confidentiality/NDAs, breach notification, audit rights, and data return in contracts.
2.3	SLA Definition	Define SLAs for patching, vulnerability disclosure, and support lifecycles.
2.4	Pre-Acceptance Validation	Require testing/validation of software/hardware prior to acceptance; document results.
2.5	Third-Party Risk Register	Maintain risk register with classification, owner, review dates, and KRIs.
2.6	Compliance Monitoring	Monitor compliance via KPIs, audits, attestations, and corrective actions.

2.7	Vendor Data Access Restrictions	Restrict vendor data access; enforce encryption and purpose limitation.
2.8	Control Alignment	Align controls to data/service criticality and classification levels.
2.9	Incident Cooperation	Establish incident cooperation and intel sharing with CERTs and regulators.
2.10	Secure Exit/Transition	Plan secure exit; revoke access, sanitize media, and return/delete data.
2.11	Subcontractor Accountability	Manage subcontractor accountability; ensure flow-down of security obligations.
2.12	Supplier Diversification	Diversify critical suppliers to reduce concentration risk; test resilience.
2.13	Risk Posture Reporting	Report supply chain risk posture regularly to the steering committee.

3) Essential Secure Software Development Life Cycle (SSDLC)

Purpose: Integrate security from requirements to operations; secure-by-design and continuous assurance.

Sr#	Sub-Point	Description
3.1	Secure by Design	Embed security requirements at design; consider privacy and classification early.
3.2	Code Review & SAST	Conduct code reviews; run SAST before merge; block builds on critical findings.
3.3	DAST & Vulnerability Scans	Execute DAST and vulnerability scans on running builds and staging environments.
3.4	SBOM & Dependency Management	Maintain SBOM for components; track CVEs; patch or replace vulnerable dependencies.
3.5	Secrets Management	Secure secrets/keys in vaults; rotate regularly; enforce least privilege in pipelines.
3.6	Environment Segregation	Segregate dev/test/prod; control releases via formal change management.
3.7	MFA Enforcement	Mandate MFA for admin tools, repositories, and CI/CD orchestrators.
3.8	Penetration Testing	Run penetration tests for internet-facing apps before go-live; fix high/critical issues.
3.9	CI/CD Security Automation	Automate security gates (linting, license check, SCA); fail non-compliant builds.
3.10	Evidence Retention	Document security testing, approvals, and exceptions; retain evidence.
3.11	Developer Training	Train developers on OWASP and platform-specific secure coding patterns.
3.12	Post-Deployment Monitoring	Monitor apps post-deploy via WAF/SIEM; capture anomalies and remediate promptly.
3.13	SSDLC Review	Review SSDLC effectiveness; improve via metrics and lessons learned.

4) Essential Security Training Controls

Purpose: Build organization-wide cyber awareness and role-based competence with measured outcomes.

Sr#	Sub-Point	Description
4.1	Training Plan	Publish a formal training plan aligned to threats and regulatory guidance.
4.2	Baseline Awareness	Mandatory baseline awareness before system access; annual refreshers.
4.3	Role-Based Modules	Provide modules for admins, developers, SOC, audit, and executives.
4.4	Delivery Methods	Deliver via e-learning, instructor-led sessions, webinars, and exercises; update content regularly.
4.5	Simulations & Drills	Run phishing simulations and tabletop IR drills; track performance.
4.6	Data Privacy	Include data privacy obligations and secure handling of sensitive information.
4.7	Remote Work Security	Cover secure remote work, mobile/BYOD, collaboration, and email hygiene.
4.8	Leadership Education	Educate leadership on risk appetite, tolerance, and oversight responsibilities.
4.9	Training Records & Metrics	Maintain training records; measure effectiveness; remediate weak areas.
4.10	Onboarding & Recertification	Require onboarding training for joiners and recertification for privileged roles.
4.11	External Expertise	Engage CERT/external experts for specialized topics where needed.
4.12	Lessons Learned Integration	Integrate lessons learned from incidents/audits into curricula.
4.13	KPI Reporting	Report training KPIs to governance; drive continuous improvement.

5) Physical Security Controls

Purpose: Protect facilities, server rooms, and infrastructure against unauthorized access and hazards.

Sr#	Sub-Point	Description
5.1	Perimeter Security	Implement fencing, guards, CCTV, access controls, and maintain visitor logs.
5.2	Sensitive Area Access	Control entry to sensitive areas; maintain audit trails and review access rights regularly.
5.3	Cabling Management	Separate and label power/data cabling; schedule inspections to prevent hazards.
5.4	Environmental Protections	Apply fire suppression, temperature, and humidity controls.
5.5	Tamper-Evident Measures	Use tamper-evident racks and seals; verify integrity periodically.
5.6	Clean-Desk & Media Control	Enforce clean-desk and media control policies for confidential materials.
5.7	Asset Tagging & Inventory	Tag assets; perform inventories and reconcile discrepancies.
5.8	Physical Security SOPs	Document physical security SOPs; review after incidents or changes.
5.9	Emergency Response Drills	Test emergency response and evacuation; record drill outcomes.
5.10	SOC Integration	Integrate physical alerts with SOC where feasible; correlate with logical events.

5.11	CCTV & Access Log Retention	Retain CCTV/access logs per policy; ensure secure storage.
5.12	Custodian Assignment	Assign custodians/owners for areas and assets; audit compliance.
5.13	Media Destruction/Reuse	Secure destruction/reuse of media; remove storage before external repair.

6) Essential Incident Response Controls

Purpose: Detect, respond, recover, and learn from incidents with clear governance and evidence.

Sr#	Sub-Point	Description
6.1	Incident Response Plan (IRP)	Publish an IRP with roles, severity taxonomy, escalation paths, and contact lists.
6.2	SOC/SIEM Monitoring	Enable SOC/SIEM monitoring; triage and validate incidents promptly.
6.3	Containment & Recovery	Execute containment, eradication, and recovery per playbooks; verify restoration.
6.4	Forensic Evidence Preservation	Preserve forensic evidence; maintain chain-of-custody; engage experts when needed.
6.5	Regulatory Notifications	Notify sectoral CERT/regulator within 72 hours of CII breaches; follow legal thresholds.
6.6	Breach Communication	Communicate to affected individuals for personal data breaches with guidance.
6.7	Stakeholder Coordination	Coordinate stakeholders; maintain status reporting and situation updates.
6.8	Root-Cause Analysis	Perform root-cause analysis; track corrective actions to closure.
6.9	IR Exercises	Run regular exercises (red/blue, tabletop); address findings.
6.10	Threat Intel Integration	Integrate threat intel sharing with CERTs and partners; update detections.
6.11	Metrics & Reporting	Measure MTTD/MTTR, recurrence, impact; report metrics to leadership.
6.12	Lessons Learned	Capture lessons learned; adjust policies, controls, and training.
6.13	IR Governance Alignment	Align IR governance to BCP/DR objectives and audit oversight.

7) Essential Identity & Access Mgmt. Controls:

Purpose: Control identities and permissions throughout the lifecycle with least privilege and assurance.

	Sub-Point	Description
7.1	JML Process	Define Joiner-Mover-Leaver processes with approvals; remove access within SLA after termination.
7.2	Role-Based Access & SoD	Implement role-based access and segregation of duties checks; document access matrices.
7.3	MFA Enforcement	Mandate MFA for remote, admin, and external access scenarios.
7.4	Access Review & Recertification	Review and recertify access periodically; prioritize high-risk roles and systems.
7.5	Privileged Account Governance	Govern privileged accounts via vaulting, session monitoring, and just-in-time (JIT) access.
7.6	Credential Security	Secure credential storage; rotate secrets; enforce strong authentication.
7.7	Access Logging	Log access requests, approvals, and changes; maintain auditable trails.
7.8	IAM Automation	Integrate IAM with HR systems for automated provisioning and deprovisioning.

7.9	Context-Aware Access	Apply time-bound and context-aware access where appropriate.
7.10	Classification-Based Decisions	Tie access decisions to asset classification and data sensitivity.
7.11	Access Hygiene Campaigns	Run access hygiene campaigns; remediate exceptions swiftly.
7.12	IAM Evidence Retention	Retain IAM logs and evidence per audit requirements; protect against tampering.
7.13	IAM KPI Reporting	Report IAM KPIs such as provisioning time, recertification exceptions, and privileged session counts.

8) Essential Governance Controls

Purpose: Establish accountable oversight, resources, and policy framework for cybersecurity.

Sr#	Sub-Point	Description
8.1	Cybersecurity Steering Committee	Form a cybersecurity steering committee led by top management.
8.2	Leadership Designation	Designate CIIO/CISO/CIO (BS-20 equivalent) as function lead with authority.
8.3	Independent Cybersecurity Function	Create an independent cybersecurity function separate from IT/ICT operations.
8.4	Roles & RACI	Define roles and RACI; document responsibilities across data, systems, and processes.
8.5	Regulatory Notifications	Notify regulators/CERTs of material changes within 30 days as per mandated timelines.
8.6	Frameworks & Policies	Maintain sector-specific frameworks and policies with implementation plans.
8.7	Risk Assessments	Conduct formal risk assessments; prioritize controls by criticality and CIA impact.
8.8	Strategy & Compliance Reviews	Approve strategy roadmaps; review against laws/regulations periodically.
8.9	Budget & Resources	Allocate budget/resources; hire qualified, experienced cyber professionals.
8.10	Culture & Accountability	Promote culture via leadership messaging, training, and accountability.
8.11	Reporting Cadences	Establish reporting cadences to management and oversight bodies.
8.12	External Linkages	Engage national/international linkages for standards and threat updates.
8.13	Governance Alignment	Align governance with nCERT/NTISB guidance and audit expectations.

9) Essential Data Collection & Privacy Controls

Purpose: Protect personal/sensitive data through lawful, transparent, and secure processing.

Sr#	Sub-Point	Description
9.1	Purpose Limitation & Consent	Limit collection to stated purposes; obtain informed consent where required.
9.2	Processing Records & Ownership	Maintain records of processing and lawful bases; assign accountable owners.
9.3	Privacy Impact Assessments (PIAs)	Conduct PIAs for new systems/projects; mitigate identified risks.
9.4	PII Access Controls	Implement access controls and monitoring for PII processing activities.

9.5	Subject Rights Workflows	Provide workflows for access, correction, deletion requests and issue notices.
9.6	Data Retention & Disposal	Apply retention limits; securely dispose of data per policy and law.
9.7	Secure Data Transfers	Secure data transfers; encrypt; use approved channels and jurisdictions.
9.8	Third-Party Agreements	Execute DPAs/NDAs with third parties; require equivalent protections.
9.9	Privacy Training	Train staff on privacy obligations and secure data handling.
9.10	Privacy Audits	Audit privacy processes; remediate deviations; record evidence.
9.11	Compliance Documentation	Document and retain compliance artifacts for regulators/auditors.
9.12	Policy Alignment	Align privacy policy with PISF 2025 and national legal requirements.
9.13	KPI & Incident Reporting	Report privacy KPIs and incidents to governance/steering committee.

10) Critical Information Infrastructure Protection (CIIP)

Purpose: Ensure continuity and resilience of essential services with sectoral oversight and CERT linkages.

Sr#	Sub-Point	Description
10.1	Continuity Focus	Focus on continuity of critical services; reduce impact of environmental, natural, and cyber threats.
10.2	BCP/DR Objectives	Develop BCP/DRP with roles, MTD, RTO, RPO; align backup strategies to these objectives.
10.3	Standards Alignment & Validation	Align plans to global standards; perform regular drills and audits for validation.
10.4	Supply Chain Assessments	Conduct supply chain risk assessments; require pre-procurement testing.
10.5	Annual Audits	Perform annual internal/external audits for sector compliance and oversight.
10.6	Change-Triggered Audits	Audit after material changes in design, configuration, security, or operations.
10.7	Confidentiality SOPs	Develop confidentiality SOPs to protect assets and data implementations.
10.8	Incident Management Structure	Structure incident management with swift detection, coordination, and reporting.
10.9	CERT Liaison	Liaise with organizational, sectoral, and national CERTs (nCERT).
10.10	CII Breach Reporting	Report CII breaches to sectoral CERT within 72 hours with clear criteria.
10.11	Threat Intel & Escalation	Share threat intelligence and breach information; define escalation paths.
10.12	National/International Linkages	Maintain national and international linkages for knowledge sharing and updates.
10.13	CIIP Metrics & Leadership Briefings	Track CIIP readiness metrics; brief leadership on residual risks and improvements.

11) Essential Audit Controls

Purpose: Strengthen governance through independent audits and continuous improvement.

Sr#	Sub-Point	Description
11.1	Internal & External Audits	Establish internal audit with at least annual audits; external oversight annually.
11.2	Control Self-Assessment (CSA)	Adopt CSA for proactive, continuous compliance.
11.3	Audit Preparation	Prepare audits with defined roles, responsibilities, and communication channels.
11.4	Auditor Selection	Select independent, certified auditors via transparent criteria.
11.5	Data Protection during Audits	Enforce NDAs; apply technical safeguards (masking/watermarking) to sensitive data.
11.6	Risk-Driven Audits	Initiate audits on a risk-driven basis aligned with obligations and incidents.
11.7	Audit Planning	Support each audit with a documented plan (scope, tools, timelines, resources).
11.8	Mandatory Documentation	Provide mandatory documents (SoA, RTP, approved Scope); ensure accuracy and up-to-date.
11.9	Evidence Integrity	Base findings on verifiable, sufficient, securely stored evidence; ensure traceability.
11.10	Observation Analysis	Analyze observations against security baselines; classify severity systematically.
11.11	Reporting & Retention	Report results in standardized formats; communicate and retain per policy.
11.12	Formal Closure	Mandate formal closure, confirm corrective actions and record lessons learned.
11.13	Continuous Improvement	Continuously improve the audit framework to reflect evolving threats and regulations.

12) Essential Risk & Management Controls

Purpose: Identify, evaluate, treat, and monitor risks with clear appetite, tolerance, and assurance.

Sr#	Sub-Point	Description
12.1	Asset & Threat Identification	Identify assets, vulnerabilities, and threats to build a comprehensive risk profile.
12.2	Risk Evaluation	Evaluate risks by likelihood and impact (including CIA); categorize levels.
12.3	Risk Register	Record risks in a register with owners, treatments, and review frequencies.
12.4	Risk Treatment Strategies	Implement strategies: mitigate, accept, transfer, or avoid with deadlines.
12.5	Continuous Monitoring	Continuously monitor risks, controls, and KRIs (incidents, downtime, penalties).
12.6	Risk Appetite Statements	Define explicit risk appetite statements per category; approve by leadership.
12.7	Tolerance Thresholds	Set measurable tolerance thresholds and escalation criteria; enforce consistently.
12.8	Responsibility & Auditability	Assign responsibilities for maintaining appetite/tolerance policies; ensure auditability.
12.9	Residual Risk Tracking	Track residual risk and control effectiveness; update register regularly.
12.10	Risk reporting integration	Integrate risk reporting with governance, audit, and strategic reviews.
12.11	Regulatory alignment	Align risk processes with sector policies and regulatory expectations.

12.12	Evidence retention	Maintain evidence of assessments, treatments, and metrics to support assurance.
12.13	Framework review & improvement	Review the framework periodically; mature via metrics and lessons learned.

13) Essential Data Center Controls

Purpose: Secure hosting environments with layered defenses and operational assurance.

Sr#	Sub-Point	Description
13.1	Physical security	Implement physical security: access control, CCTV, visitor management, and guard SOPs.
13.2	Network security controls	Deploy NGFW, WAF, IDS/IPS, DDoS protection, DLP, and DMZ segmentation.
13.3	Server & platform hardening	Harden servers and platforms with standard secure configurations.
13.4	Patch & vulnerability management	Maintain patching and vulnerability scanning; prioritize remediation based on risk.
13.5	SIEM/SOC operations	Operate SIEM/SOC for real-time detection, response, and threat hunting.
13.6	Cabling management	Manage cabling formally: labeling, separation of power/data, and periodic inspections.
13.7	Log retention	Retain comprehensive logs and audit trails for ≥12 months on critical systems.
13.8	Internal & external audits	Conduct internal audits and annual third-party audits for assurance and compliance.
13.9	BCP/DR alignment	Align BCP/DRP to service criticality; test and update plans regularly.
13.10	Data center compliance	Migrate to compliant in-country data centers when minimum controls are unmet.
13.11	Documentation & evidence	Document SOPs, runbooks, and evidence; align to regulatory frameworks.
13.12	Ownership assignment	Assign clear ownership across operations, security, and compliance functions.
13.13	Governance reporting	Report posture and gaps to governance; track remediation to closure.

PISF Mapping Chart

The framework defines 38 mandatory actions, structured across product, service, and policy dimensions, to achieve full compliance with the PISF standard.

Total Scoring Audit			20	2	1	2	5	1	1	1	1	1	1	2
Phase #	**Control Name**	**Sub-Point**	Policy	3rd Party Audit	FW	EPP	SIEM	SOC	Vul Ass.	VAPT	Back up	Phys Sec	Training	IAM
Phase 01	Essential Governance Controls	A. Policies and Procedures	✓											
		B. Leadership and Commitment	✓											
		C. Organizational Structure	✓											
		D. Change Management	✓											
		E. Compliance and Third-Party Management		✓										
Phase 02	Essential Risk & Management Controls	A. Asset Management	✓											
		B. Software and License Management	✓											
		C. System Categorization and Classification	✓											
		D. Risk Management	✓											
Phase 03	Essential System & Communication Protection Controls	A. Network Security			✓									
		B. Protection of Endpoint Computing Devices				✓								
		C. Event Logs and Monitoring					✓							
		D. Backup and Recovery Management									✓			
		E. Vulnerability and Patch Management							✓					
	Essential Supply Chain Controls	A. Supply Chain Life Cycle Management	✓											
		B. Supply Chain Risk Management	✓											
	Essential Secure Software Development Life Cycle (SSDLC)	A. Essential SSDLC Controls	✓											
	Essential Physical Security Controls	A. Physical Security Controls												✓

	Essential Incident Response Controls	A. Incident Management					✓						
		B. Incident Response					✓	✓					
		C Business Continuity Plan	✓										
		D. Disaster Recovery Plan	✓										
	Essential Identity & Access Management (IAM) Controls	A. Identity and Access Management											✓
		B. Privileged Access Management											✓
	Essential Data Collection & Privacy Controls	A. Data Privacy	✓										
		B. Data Security				✓	✓						
		C. Data Breach	✓										
	Essential Datacenter and Web Hosting Services Controls	A. Datacenter	✓										
		B. Email and Web Hosting Services	✓										
		C. Web Application Security							✓				
	Critical Information Infrastructure Protection (CIIP)	A. Governance & Resource Allocation	✓										
		B. Critical Asset Classification Framework	✓										
		C. CIA - Aligned Con	✓										
Phase 04	Essential Audit Controls	A. Cybersecurity Audit		✓									
Phase 05	Essential Security Training Controls	A. Essential Security Training Controls										✓	

Abbreviations

Abbreviation	Complete Term
Policy	Policy Framework
3rd Party Audit	Third-Party Audit
FW	Firewall
SIEM	Security Information and Event Management

Abbreviation	Complete Term
SOC	Security Operations Center
Vul Ass	Vulnerability Assessment
Backup	Backup
VAPT	Vulnerability Assessment and Penetration Testing

Abbreviation	Complete Term
Training	Training
Phy Sec	Physical Security
EPP	Endpoint Protection Platform
IAM	Identity and Access Management

About Cyber Silo

CyberSilo is Pakistan's fastest-growing cybersecurity company, having offices in US, Pakistan and Canada serving customers in more than **10+ countries and 4 regions**. We deliver cutting-edge solutions including **SIEM, SOAR, Threat Intelligence, Vulnerability Assessment, Infrastructure Hardening Tools, and VAPT services**; empowering organizations to strengthen resilience, achieve compliance, and stay ahead of evolving cyber threats.

What Cybersilo Offers

Service Area	Scope & Alignment with PISF 2025
Free Gap Assessment	Benchmark your current posture against PISF 2025 and international standards, with a clear roadmap of strengths, weaknesses, and priority actions.
Cybersecurity Tools	We deliver cutting-edge solutions including **SIEM, SOAR, Threat Intelligence, Vulnerability Assessment, Infrastructure Hardening Tools, and VAPT services**
Threat Exposure Management	Integrate threat intelligence, vulnerability management, and incident playbooks for proactive defense.
Training & Awareness	Deliver role-based training modules, phishing simulations, and leadership education aligned with mandatory awareness programs.
Strategic Advisory	Align cybersecurity governance with business objectives, regulatory expectations, and sectoral CERT reporting obligations.

Contact for Gap Assessment

- Abdul Moiz Arif | Gap Assessment & Advisory
- moiz@cybersilo.tech
- +92 334 4556556