

PISF 2026 Framework Implementation Timelines

1. Executive Summary & Core Implementation Principle

The implementation of the Pakistan Information Security Framework (PISF) shall be guided by the principle that organizational maturity determines the pathway and pace of implementation. This document recognizes that entities possess varying baseline capabilities, governance structures, and technical resources. Organizations shall adopt a risk-based, phased roadmap that prioritizes the establishment of fundamental capabilities before progressing to the full spectrum of framework controls.

2. Progressive PISF Implementation

Progressive implementation should generally follow the sequence below:

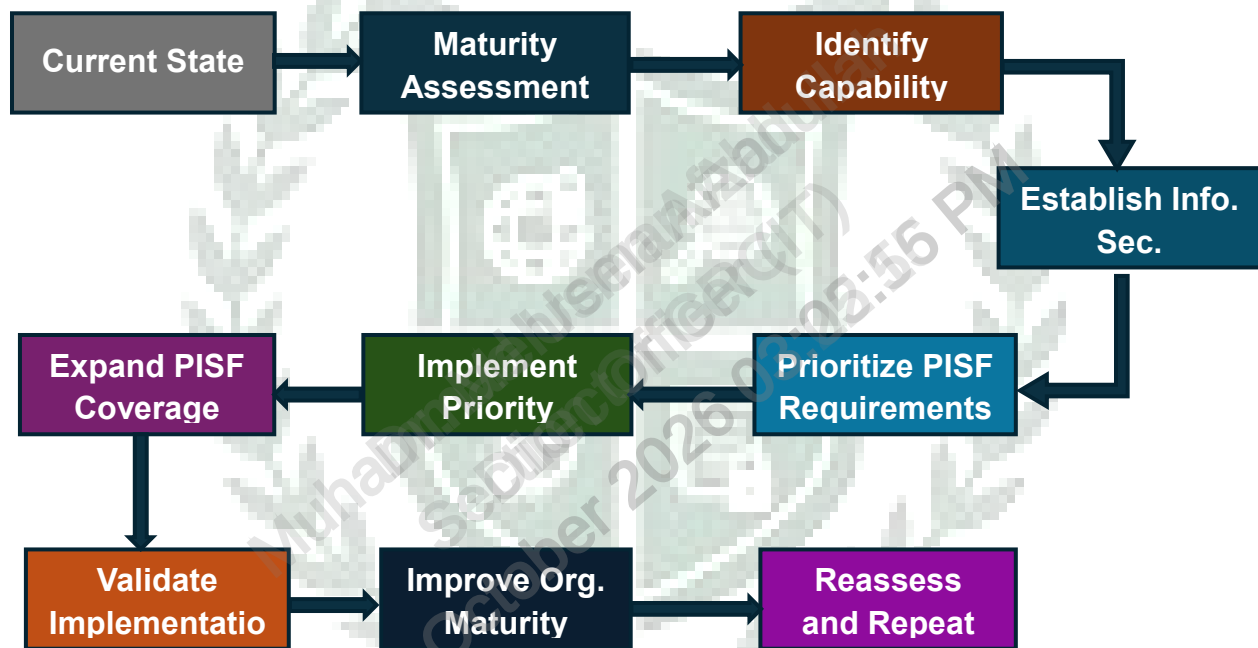


Figure 1: Progressive Implementation Pathway for PISF

The organization should periodically reassess its maturity and implementation status and update its roadmap accordingly.

3. Organizational Maturity Assessment Methodology

Organizational maturity shall be assessed across eight objective parameters, applying a **0–3 scoring scale** with a maximum attainable score of **24**. The Maturity Assessment shall determine the institution's capacity to sustain and operationalize security functions on a continuing basis. The resulting maturity score shall constitute the definitive benchmark for evaluating organizational readiness, resilience, and progression through the phased implementation of the Pakistan Information Security Framework (PISF). The table below sets out the parameters, assessment considerations, and scoring scales that shall be applied in determining organizational maturity under the Pakistan Information

Security Framework (PISF)

Parameter Name	Assessment Considerations & Governance Focus	Detailed Scoring Scale (0–3)
InfoSec Governance	Formal reporting lines, oversight committees, CISO/InfoSec Lead accountability structures, and defined roles.	0: Non-existent 1: Initial (Informal) 2: Established (Formal) 3: Mature (Integrated)
GRC Team	Availability of qualified GRC Lead, dedicated GRC analysts, and technical security engineers.	0: No dedicated staff 1: Informal/handled by general IT 2: Formal security resources exist 3: Mature, fully integrated team
Policies & Procedures	Existence, formal approval, communication, enforcement, and periodic lifecycle reviews.	0: No formal policies 1: Drafts exist but fragmented 2: Formally approved, implemented & communicated 3: Consistently reviewed & optimized
Risk Management	Formal risk assessments, risk registers, mitigation plans, acceptance, and active monitoring.	0: No risk process 1: Ad-hoc/informal assessments 2: Formal register & treatments 3: Monitored continually
InfoSec Framework	Adoption and operationalization of any Framework like ISO/IEC 27001, CTDISR or equivalent formal ISMS.	0: No framework adoption 1: Partial or informal adoption 2: Formally adopted & compliant 3: Fully integrated & Certified
Technical Capability	Availability and effectiveness of technical controls and capabilities across the organization such as access control, vulnerability management, backup, security monitoring, endpoint protection, network security, and other applicable controls.	0: Core controls absent 1: Inconsistent/fragmented controls 2: Standard controls generally enforced 3: Automated & quantitatively measured
Internal and external / third-party Audit	Internal audits, vulnerability assessments, penetration testing, and management reviews.	0: No internal / external audits 1: Ad-hoc/inconsistent checks 2: Regular, formal audit capability 3: Continuous compliance monitoring & audits
Awareness & Improvement	Security awareness training, role-based training, lessons learned and continuous improvement.	0: No awareness training 1: Dependent on individual initiative 2: Formal training program

		exists 3: Integrated security training culture.
--	--	--

4. Maturity Score

The overall maturity score shall be determined as the aggregate of scores assigned across the eight parameters, with the maximum attainable score being 24. The overall score shall not be applied in isolation. For compliance purposes, organizations shall be required to demonstrate adherence to the minimum capability conditions prescribed for each maturity tier, ensuring that advancement through the Pakistan Information Security Framework (PISF) is based on both cumulative scoring and fulfillment of baseline capability requirements.

The following table sets out the prescribed minimum capability conditions required for classification under each maturity tier of the Pakistan Information Security Framework (PISF).

Table 1: Minimum Capability Conditions

Tier	Score	Starting Capability Profile	Minimum Conditions / Strategy
Tier 1: Foundational	0 – 8	Limited capability; security handled ad-hoc.	Must execute a Capability Establishment Stage prior to full PISF phases.
Tier 2: Developing	9 – 16	Security staff exist, but risk management is fragmented.	Strengthen existing governance, formalize integrated risk management.
Tier 3: Established	17– 24	Dedicated CISO, mature ISMS, robust technical controls.	Targeted gap closure, continuous monitoring & improvements.

5. PISF Implementation Timeline

The following section outlines the phased timeline through which organizations shall implement the Pakistan Information Security Framework (PISF), aligned with their assessed maturity tier and minimum capability conditions.

Phase	Tier 3: Established (12 Months)	Tier 2: Developing (15 Months)	Tier 1: Foundational (18 Months)
Phase 1: Maturity Assessment & Governance	1 Month	2 Months	3 Months
Phase 2: Asset Inventory / Risk Assessment / Gap Assessment (PISF)	2 Months	3 Months	4 Months

Phase 3: Implementation of Security Solutions & Policies (PISF)	7 Months	8 Months	9 Months
Phase 4: Internal Audit & Vulnerability Assessment (PISF)	2 Months	2 Months	2 Months
Total Timeline	12 Months	15 Months	18 Months
Note: Entities operating at significant scale (including but not limited to organizations with more than 500 nodes, geographically dispersed departments) or subject to budgetary and procurement constraints or other organizational challenges may, upon formal justification, be granted an extension of three to six months beyond the prescribed maturity-based implementation timeline. Such extension shall be duly documented and shall require prior approval from the competent executive authority of the organization.			



Figure 2: Phased PISF Implementation Timelines Across Maturity Tiers

Note: In circumstances where an organization lacks the requisite internal human resource capacity or specialized security expertise, such entities may obtain professional support through PKCERT-authorized firms and accredited consultants.

Furthermore, the timeframes allocated to individual implementation phases may be adjusted in accordance with organizational constraints or specific requirements, provided that the overall duration remains consistent with the maturity-based timeline as assessed. Any such adjustments shall be formally recorded and subject to approval by the competent executive authority.

6. Risk Prioritization & Continual Improvement

- Control Prioritization:** Implementation must be prioritized based on asset criticality, business impact, legal/regulatory mandates, active vulnerabilities, and resource availability. Deferred controls must be formally documented with risk acceptance and target closure dates.
- Continual Reassessment:** PISF compliance is an ongoing lifecycle. Organizations must conduct periodic dual assessments measuring both PISF Gap Closure and Organizational Maturity Growth to drive iterative capability maturity.