PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

NTISB

A. INTRODUCTION

1. **"Pakistan Information Security Framework (PISF)"**, outlines the baseline of information security controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs. This framework establishes mandatory baseline information security controls for federal departments to ensure compliance with applicable information security implementation requirements issued by NTISB and nCERT in accordance with the "*National Cyber Security Policy 2021*" and the *CERT Rules 2023*.

2. PISF is comprised of following 13 documents:

(1) Essential Governance Controls

(2) Essential Asset and Risk Management Controls

(3) Essential Security Training Controls

(4) Essential System and Communication Protection Controls

(5) Essential Identity and Access Management Controls

(6) Essential Data Protection and Privacy Controls

(7) Essential Incident Response Controls

(8) Essential Physical Security Controls

(9) Essential Data Centre and Web Hosting Services Controls

(10) Essential Secure Software Development Life Cycle Controls

(11) Essential Supply Chain Management Controls

(12) Essential Audit Controls

(13) Essential CII Protection Controls

B. APPLICABILITY

3. This framework shall be applicable to all Federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

4. Throughout the document, the term "organization" will be used to refer any of the above.

5. Scale and size of the implementation will vary according to the size of the organization.

C. PISF IMPLEMENTATION ROAD MAP

6. The implementation roadmap outlines a phased approach to establish and maintain a robust security posture across the organization:

7. **Phase 1 - Essential Governance Controls:** Define policies, standards, procedures, roles, responsibilities and oversight mechanisms to establish the foundation for essential security.

8. **Phase 2 - Essential Asset & Risk Management Controls:** Identify and evaluate critical assets through risk assessment process and devise controls for effective risk management.

9. **Phase 3 - Essential Core Controls:** System and communication protection, identity and access management, data protection and privacy, incident response, physical security, supply chain management and continuous monitoring constitute the foundational security controls that every organization shall implement.

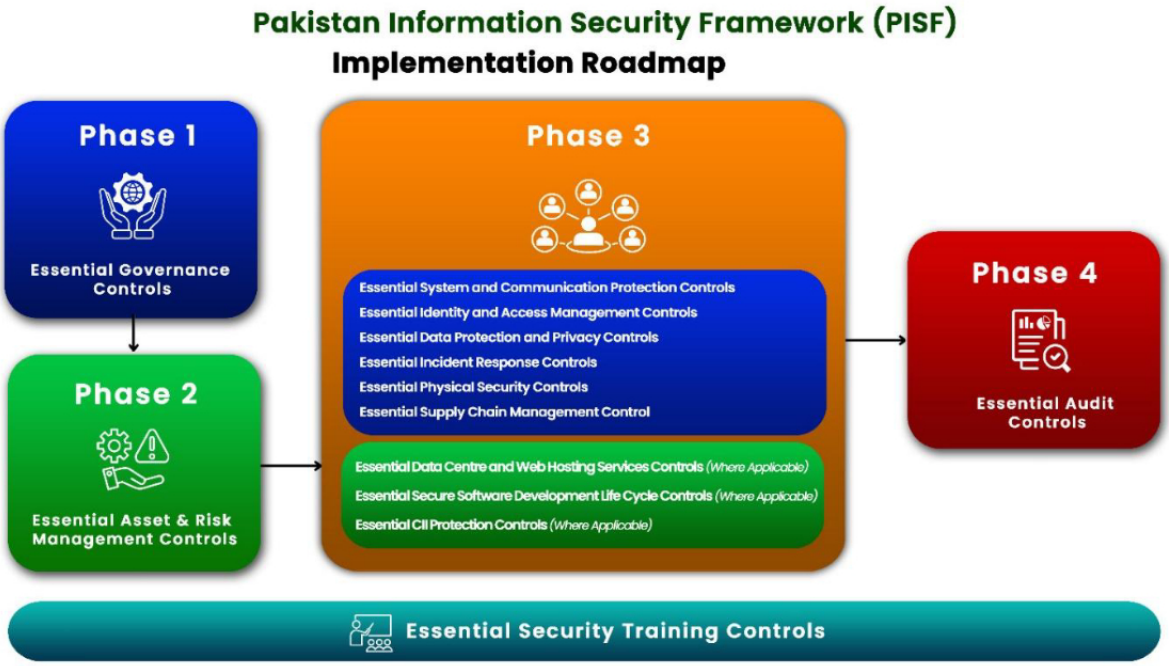
10. **Phase 4 - Audit Controls:** Audit validate compliance, assess effectiveness of processes and controls, and drive continual improvement through structured processes.

11. **Security Training:** Training programs are embedded into each of the above-mentioned phase to ensure that employees have the knowledge and capabilities to effectively implement and sustain essential security controls.

12. **Data Center and Web Hosting Services:** Applicable to organizations that operate their own data centers or utilize/provide web hosting services.

13. **Secure Software Development Life Cycle (SSDLC):** Applicable to organizations engaged in software design, development, or maintenance activities.

14. **Critical Information Infrastructure (CII) Protection:** Applicable to organizations or sectors designated as critical information infrastructure.



D. COMPLIANCE CRITERIA

15. This framework adopts a structured compliance assessment approach to ensure consistent evaluation and reporting across all

applicable controls. The compliance criteria are presented through two complementary tables.

a) The table-1 defines the applicability of each control by determining whether it is In Scope or Out of Scope of the organization's Information Security Management System (ISMS), based on organizational context, processes, systems, and risk exposure.

Table 1: In scope and Out of Scope Detail

Options	Description	When to Select
In Scope	The control is applicable to the organizations information security Management System (ISMS). It addresses a process, asset or risk relevant to your environment.	Select this when the control is relevant to your organization operations or information security requirements.
Out of Scope	The control is not applicable to the organization's ISMS. It does not impact or relate to any process, system, or data within your defined ISMS boundaries.	Select this when the control does not apply due to the organization's context, structure, services, or operations.

b) The Table *2* assesses the level of control implementation using defined maturity levels, ranging from **Not Compliant** to **Fully Compliant**, to reflect the extent to which controls are implemented, documented, and effectively operated. Together, these tables enable a clear, auditable, and risk-informed view of control applicability and implementation maturity, supporting regulatory compliance, continuous improvement, and informed management oversight.

Note: All controls derived from PISF will be published as Annexure of this Framework.

Table 2: Compliance Criteria

Options	Description	When to Select
Not Compliant	The control is not implemented or is completely missing. There are no procedures, evidence, or actions in place to meet the control's requirements.	Select this when no implementation or documentation exists for the control.
Partially Compliant	The control is partially implemented, but there are gaps in documentation, consistency, or coverage. Some evidence exists, but it does not fully meet Control requirements.	Select this when initial work has started, but further improvement or completion is needed.
Mostly Compliant	The control is largely implemented, with minor gaps or areas for improvement. Most of the required measures and evidence are in place.	Select this when the control is effectively applied but not yet perfect or fully documented.
Fully Compliant	The control is fully implemented and meets Control requirements. Documentation, evidence, and practices are complete, effective, and regularly reviewed.	Select this when the control is mature and consistently followed and regularly reviewed across the organization.

PKCERT

Safeguarding Pakistan's Cyberspace

info@pkcert.gov.pk
www.pkcert.gov.pk