National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Governance Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework 2025: **"Essential Governance Controls"**, outlines the baseline of information security governance controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all employees and third parties, establishing the organization's approach to information security by defining governance, compliance requirements, and management responsibilities to ensure consistent protection of information and systems.

B. PISF IMPLEMENTATION ECOSYSTEM

3. **Financial Planning:** Organizations shall allocate dedicated funds for cybersecurity solutions, training, certification and audits in their annual budget, tailored to their specific needs.

4. **Human Resource Development:** Organizations shall fulfill cybersecurity staffing requirements by converting redundant, vacant, or underutilized positions into dedicated cybersecurity roles

5. **External Expertise:** Organizations lacking internal expertise may outsource cybersecurity services like consultancy, risk assessment, and audits to nCERT/ Regulator/ Sectoral CERT registered firms via PPRA-compliant bidding processes.

6. **Oversight and Compliance:** Oversight audits shall be performed by nCERT/ NTISB, sectoral CERTs and Regulator for compliance assessment.

C. ORGANIZATIONAL STRUCTURE

7. The Head of the organization, principal accounting officers, or the governing board of the organization shall be ultimately responsible and accountable for security governance, risk management, compliance, and cyber risk oversight.

8. A steering committee for cyber/ info security matters shall be formulated and notified headed by the top management of the organization, responsible for making strategic direction, prioritization, and oversight of cyber/ info security-related decisions.

9. A dedicated cyber/ information security function/team (e.g., Wing, department, branch tailored to the organization context) shall be established. This function shall be independent from the Information Technology/Information Communication and Technology (IT/ICT), reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest with IT/ ICT.

10. The organization shall designate a cyber / information security function lead (e.g., CISO, CIO, CRO, BS-20 or equivalent) who shall be a member of the organization's steering committee responsible for technology-related decision-making.

11. Steering committee shall define, document, approve, and assign cybersecurity roles, and responsibilities, ensuring no conflict of interest arises from these assignments.

12. RACI matrix (Responsible, Accountable, Consulted, and Informed) for all data, systems and processes shall be maintained.

13. The roles of cyber/ info security function lead, along with associated supervisory and critical positions within the function, are

required to be filled by full-time, experienced cybersecurity professionals.

14. Organizations shall ensure that Information Security and IT personnel are dedicated to their core functions and are not assigned to non-IT administrative or support roles, to maintain focus on security and technical responsibilities.

15. The cyber/ info security steering committee shall provide regular reports to top management to ensure informed decision-making and alignment with organizational risk management strategies.

16. The organization shall establish governance over incident management by ensuring that all security incidents are reported, managed in accordance with the incident response plan, and aligned with business continuity objectives.

17. The organization shall ensure that internal and external audits are conducted, review and address audit outcomes, implement corrective actions, and maintain complete audit records and documentation.

D. POLICIES AND PROCEDURES

18. The cyber/ info security function shall be responsible for defining, documenting, and implementing cybersecurity policies and procedures. These policies and procedures shall be approved by the steering committee and subsequently disseminated to relevant stakeholders.

19. The cyber/ info security policies and procedures must be aligned with the organization objectives, information security objectives, and framework & guidelines issued by nCERT/ Sector Regulator from time to time.

E. LEADERSHIP AND COMMITMENT

20. Head of the organization or Top management shall demonstrate leadership and commitment with respect to the information security by ensuring the following:

(a) A cybersecurity strategy shall be formulated. The strategy goals shall be in-line with relevant laws and regulations.

(b) A roadmap shall be executed to implement the cybersecurity strategy and reviewed periodically according to planned intervals or upon change in relevant laws, regulations and guidelines.

(c) An organizational structure shall be established supporting information security governance and operations, ensuring availability of skilled human resources, planning and allocation of sufficient financial resources for effective information security operations.

(d) Senior management shall oversee information security initiatives by emphasizing their significance, mandating comprehensive security training, verifying effectiveness, guiding personnel, fostering continuous improvement, and supporting cyber/ info security teams in establishing a resilient security posture that aligns with the organization's risk profile and sensitivity levels.

F. CHANGE MANAGEMENT

21. The organization shall ensure that all changes to information systems, applications, infrastructure, configurations, and security controls shall be formally managed through an approved change management process.

22. Proposed changes shall be assessed by the cyber/ info security function for information security risks, compliance impacts, and potential effects on business operations prior to implementation.

23. No change shall be implemented without appropriate authorization, based on defined roles and responsibilities, and in accordance with organizational governance structures. Only emergency changes which are required to address critical incidents or vulnerabilities shall be formally reviewed and documented after implementation.

G. COMPLIANCE AND THIRD-PARTY MANAGEMENT

24. The organization shall identify and maintain an up-to-date inventory of all applicable laws, regulations, standards, contractual obligations, and directives.

25. The organization shall designate independent internal audit function to conduct compliance assessments, manage findings, maintain records, and report key results to management.

26. The organization shall ensure third-party compliance through supplier assessments, evaluation of security compliance posture, verification of legal authorizations and controls, including data protection and security standards.

PKCERT

Safeguarding Pakistan's Cyberspace

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