National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Critical Information Infrastructure Protection (CIIP) Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework: **"Essential Critical Information Infrastructure Protection (CIIP) Controls"**, outlines the baseline of information security CIIP controls for federal and provincial government ministries and divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all entities designated as Critical Information Infrastructure (CII), including government organizations, regulators, service providers and third parties who design, manage, operate, or maintain systems and assets supporting critical services. It also covers all critical systems, applications, networks, operational technologies, and associated assets that are essential for the secure and reliable functioning of CII. It applies to the end-to-end lifecycle of infrastructure, including planning, deployment, operations, monitoring, risk management, and incident response.

B. GOVERNANCE & RESOURCE ALLOCATION

Note: Governance shall be read in conjunction with the clauses in **"Essential Governance Controls"**.

3. The implementation of information security should get adequate funding & resources, and top management should be involved in developing the structures and strategy for information security by making prompt and efficient business decisions on critical information security matters.

4. The Head of the organization, (CII Owner (CIIO)) shall be ultimately responsible and accountable for information security governance, risk management, compliance, and risk oversight.

5. If a material change is made to the design, configuration, security or operational features of the CII, CIIO shall notify its sector regulator (or CII CERT) of such changes within 30 days from the date of the completion of the change.

6. The organization shall designate an information security function lead (e.g., CISO, CIO, CRO, BS-20 or equivalent) reporting 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.

7. A steering committee for information security matters shall be formulated and notified headed by the top management of the organization, which shall be responsible for making strategic direction, prioritization, and oversight of information security and technology related decisions. Information security function lead shall be member of this steering committee.

8. Steering committee shall define, document, approve, and assign cyber/information security roles and responsibilities, ensuring no conflict of interest arises from these assignments.

9. The roles of cyber/information security function lead, along with associated supervisory and critical positions within the function, are required to be filled by full-time, qualified and experienced cyber/information security professionals.

10. 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.

11. The cyber/ information security steering committee shall provide regular reports to top management to ensure informed decision making

and alignment with organizational objectives and risk management strategies

12. The CIIO shall be responsible for ensuring that roles and responsibilities related to CII information security are documented, assigned, and clearly communicated.

13. All documented roles and responsibilities shall include appropriate authorizations and be formally approved by top management.

14. CII shall establish and maintain frameworks and policies to ensure the information security specific to its sector and services.

15. Each CII shall conduct formal risk assessments across its infrastructure through qualified and experienced professionals. Security controls should be implemented based on risk prioritization rather than ad-hoc measures.

C. CRITICAL ASSET CLASSIFICATION FRAMEWORK

16. CII shall establish a framework to categorize and classify assets as Most Critical, Highly Critical, Critical, or Non-Critical based on severity.

Table 1: Classification Scheme

Level	Impact of compromise
Most Critical	**Catastrophic**, can result in extreme safety threats, extreme financial damage, or complete business halt.
Highly Critical	**Severe** disruption of essential services, high financial damages etc., safety threats.
Critical	**Noticeable** operational issues but manageable or medium level financial damages, limited safety threats.
Non-Critical	**Minimal** operational effect, tolerable financial impact.

17. The organization may also classify assets by mapping them to confidentiality, integrity, and availability (CIA), ensuring that any unauthorized disclosure of information is recognized as having the potential to cause serious adverse impacts on operations, assets, or individuals.

Table 2: Classification mapping with Impact on CIA

Impact on CIA	Non-critical	Critical	Highly Critical	Most Critical
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and sensitive information.	The unauthorized disclosure of information could be expected to have **no specific or limited** adverse impact on operations, assets or individuals.	The unauthorized disclosure of information could be expected to have **considerable** adverse impact on operations, assets or individuals.	The unauthorized disclosure of information could be expected to have **serious** adverse impact on operations, assets or individuals.	The unauthorized disclosure of information could be expected to have **severe or catastrophic** adverse impact on operations, assets or individuals. (e.g., PII, financials).
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **tolerable or no-specific** adverse	The unauthorized modification or destruction of information could be expected to have a **considerable, noticeable** adverse impact on operations,	The unauthorized modification or destruction of information could be expected to have a **serious** adverse impact on	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse impact on operations,

	impact on operations, assets or individuals.	assets or individuals.	operations, assets or individuals.	assets or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **tolerable or no-specific** impact on operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **considerable/ noticeable** impact on operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** impact on operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** impact on operations, assets or individuals. (Unavailability may affect public safety, disruption in a 24/7 service etc.).

<u>Note:</u> For convenience or comprehension, organizations may choose to create three levels rather than four by combining critical and highly critical or highly critical and most critical into a single level. ***The organization can define its own terminologies as well (e.g. Top Secret, Secret, Confidential, Public, etc.).***

D. CIA-ALIGNED CONTROL IMPLEMENTATION

18. Implementation of information security controls should be realistic, ensuring confidentiality, Integrity and Availability (CIA) of the CII after adequate analysis of the criticality of data and services and approvals of higher management including regulator of the sector, if applicable. For allocation of resources, priority shall always be given to the assets "loss or compromise of which could result in **major detrimental impact on the availability, integrity or delivery of essential services**".

19. CIIs shall implement and regularly test all necessary information security controls including appropriate access control mechanisms according to the criticality of the asset, privileged access controls, authentication, encryption, network security controls, data security and privacy.

20. CIIs shall ensure the protection and privacy of personal data and enforce approved data retention and disposal policies in accordance with legal, regulatory, and sectoral requirements.

21. Security requirements shall be integrated during the design and development phases of any new or significantly modified CII systems or facilities following security by design and secure architecture principles.

22. CII shall establish and maintain documented policies and plans for physical and environmental security to safeguard infrastructure.

23. Protection and information security of CII shall be focused on the continuity of the critical services and focusing on reducing the likelihood and impact of any disruption caused by any environmental, natural, operational or cyber threats.

24. The organization shall develop Business continuity plan (BCP), and Disaster Recovery Plan (DRP) as a formal document with clarity of actions, roles and responsibilities, communication procedures, training requirements and drill exercises.

25. CIIs shall periodically conduct resilience and stress testing of critical infrastructure components, including power supply systems, backup generators, cooling and HVAC systems, network connectivity, and telecommunications links, to verify redundancy, failover capability, and sustained operation under adverse conditions. Test results shall be documented, reviewed, and used to improve resilience measures.

26. The organization shall establish and enforce approved recovery and response metrics (recovery time objective (RTO), Recovery Point Objective (RPO), Mean time to detect (MTTD) and Mean time to response (MTTR)) for critical systems and services to ensure effective detection, response, recovery and minimal data loss consistent with business continuity and operational resilience objectives.

27. BCP and DRP should be realistic, risk based and appropriately approved by the higher management of CII and regulator of the CII sector, wherever applicable.

28. CIIs shall perform regular backup restoration testing to verify the integrity, completeness, and recoverability of critical data and systems. CIIs shall also formally identify, document, and mitigate single points of failure (SPOFs) across systems, infrastructure, processes, and dependencies to strengthen availability and operational resilience.

29. CII shall conduct supply chain risk assessments and ensure that procurement of software, hardware, and services includes proper security testing and evaluation.

30. CII shall establish a mechanism of annual internal and external audits for ensuring compliance to the critical sector specific policies, documents, standards and policies. Regulator of the critical sector and nCERT/NTISB, as applicable, will be responsible for the external audit oversight. Audit shall also be conducted in case of any material change in design, configuration, security or operational features of the CII.

31. CIIs shall establish and enforce audit confidentiality procedures to ensure the protection of information, including system designs, configurations, and security controls.

32. CII shall adopt a structured approach for managing incidents, ensuring swift detection, response, reporting, recovery, and coordination across all relevant stakeholders:

33. CIIs shall maintain liaison with organizational CERTs, sectoral CERTs, and the national CERT (nCERT) for timely incident reporting and knowledge sharing.

34. Each CII shall develop and maintain an Incident Response Plan (IRP) detailing procedures for handling information security incidents, roles, responsibilities, escalation paths, and recovery steps.

35. Mechanisms shall be developed for sharing threat intelligence, incident data, and breach information with sectoral CERTs, with clear criteria for escalation to nCERT.

36. All information security breaches or attacks on CIIs shall be reported to the relevant sectoral CERT within **72 hours**.

37. Standard Operating Procedures (SOPs) shall define coordination and communication mechanisms between organizational, sectoral, and nCERT.

38. CIIs shall provide continuous information security awareness and role-based training for all employees, including senior officials, to reduce risks arising from human error, phishing, and social engineering attacks.

39. CII shall establish and maintain national and international linkages and cooperation mechanisms to stay updated on evolving threats, sector specific risks, global best practices, and emerging technologies.

PKCERT

PKCERT

Safeguarding Pakistan's Cyberspace

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