National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Critical Information Infrastructure Protection (CIIP) Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework 2025: **"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 cyber security should get adequate funding & resources, and top management should be involved in developing the structures and strategy for cyber security by making prompt and efficient business decisions on critical cyber security matters.

4. The Head of the organization, (CII Owner (CIIO)) shall be ultimately responsible and accountable for security governance, risk management, compliance, and cyber 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. A steering committee for cyber security matters shall be formulated and notified headed by the top management of the organization, responsible for making all cyber security related decisions.

7. 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.

8. Cyber security function lead will be directly reporting to the head of the organization.

9. A dedicated cybersecurity 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 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.

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

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

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

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

C. CRITICAL ASSET CLASSIFICATION FRAMEWORK

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

Table 1: Critical Asset Classification

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.

16. 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: Asset Classification Based on CIA Impact

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 impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **considerable, noticeable** adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse impact on operations, 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.).

***Note:** 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.*

D. CIA-ALIGNED CONTROL IMPLEMENTATION

17. Implementation of cyber 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***".

18. 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 shall be implemented and tested.

19. Data privacy and security shall be maintained, and data retention policies shall be followed.

20. Security shall be integrated during the design and development phases of any new CII system or facility (security by design).

21. CII shall establish policies and plans for physical and environmental security to safeguard infrastructure against physical threats.

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

23. Business continuity planning (BCP), Disaster Recovery Plan (DRP) shall be a formal document with clarity of actions, roles and responsibilities, training and drill exercises.

24. 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.

25. BCP should be realistic and appropriately approved by the higher management of CII and regulator of the CI sector, wherever applicable.

26. BCP/DRP shall be aligned with globally recognized standards and undergo regular testing and audits to validate effectiveness.

27. CII shall conduct supply chain risk assessments and ensure that procurement of software/hardware includes proper testing and evaluation.

28. 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.

29. To guarantee that auditors will protect the confidentiality of the assets, including data and security implementations, CII shall develop audit confidentiality SOPs.

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

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

32. Each CII shall develop and maintain an Incident Response Plan (IRP) detailing procedures for handling cyber incidents, roles, responsibilities, and recovery steps.

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

34. All cybersecurity breaches or attacks on CIIs shall be reported to the relevant sectoral CERT within **72 hours**.

35. Standard Operating Procedures (SOPs) shall define coordination processes between organizational, sectoral, and national CERTs.

36. CIIs shall provide continuous cybersecurity awareness and training for all employees, including senior officials, to reduce risks from human error, phishing, and social engineering attacks.

37. CII shall establish and maintain national and international linkages to stay updated on evolving cyber threats, global best practices, and emerging technologies relevant to their sector.

PKCERT

Safeguarding Pakistan's Cyberspace

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