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.

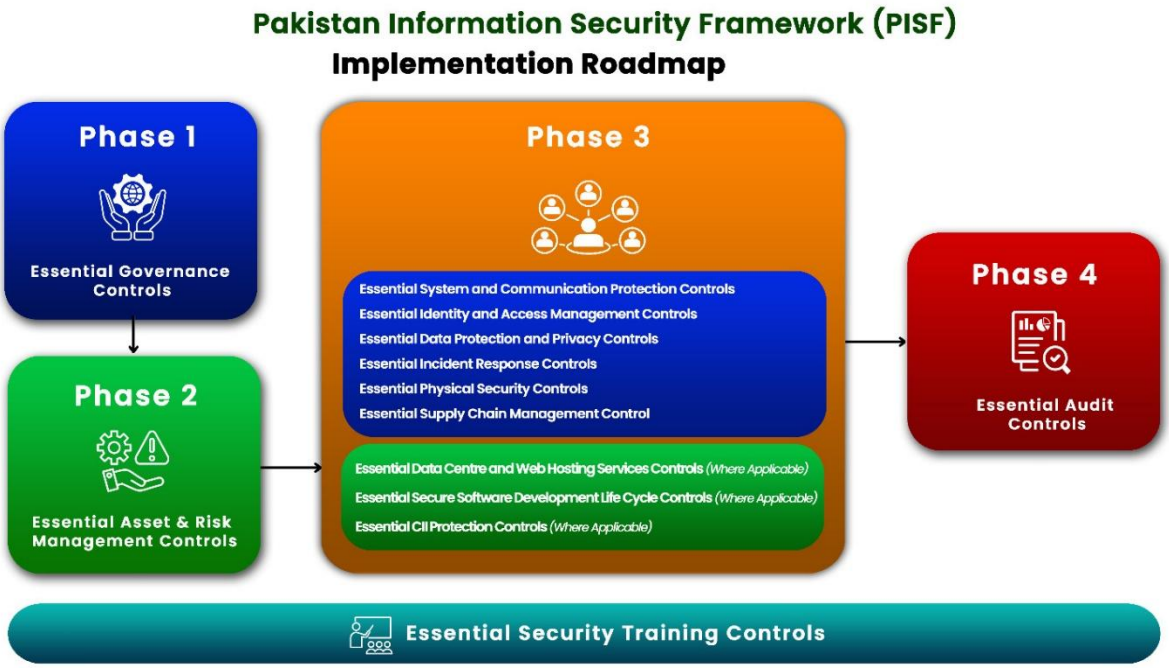
10. **Phase 4 - Audit Controls:** Audit validate compliance, assess effectiveness of processes and controls, and drive continual improvement through structured processes.

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Governance Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework: **"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, contractors 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 information security solutions, training, certification and audits in their annual budget, tailored to their specific needs.

4. **Human Resource Development:** Organizations shall fulfill information security staffing requirements by either converting redundant, vacant, or underutilized positions into dedicated information security roles or hiring of new resources appropriate for such position.

5. **External Expertise:** Organizations lacking internal expertise may outsource information security 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 information security governance, risk management, oversight and compliance.

8. 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).

9. The organization shall designate a 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.

10. 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.

11. Steering committee shall define, document, approve, and assign cyber/information security 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 documented and maintained.

13. 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.

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/ 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.

16. The organization shall establish governance for 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 establish proactive monitoring mechanism for its information system assets and security controls. It will help in continuous assessment of organization's security posture, maintaining risk profile and will support top management for informed decisions.

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

D. POLICIES AND PROCEDURES

19. The cyber/information security function shall be responsible for defining, documenting, and implementing information security policies and procedures. These policies and procedures shall be approved by

the steering committee and subsequently disseminated to relevant stakeholders.

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

E. LEADERSHIP AND COMMITMENT

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

(a) An information security strategy shall be formulated. The strategy goals shall be in-line with relevant laws and regulations.

(b) A roadmap shall be devised and executed to implement the information security 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/information security teams in establishing a resilient security posture that aligns with the organization's risk profile and sensitivity levels.

F. CHANGE MANAGEMENT

22. 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 and procedure.

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

24. 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

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

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

27. The organization shall ensure third-party compliance through supplier assessments, audits, evaluation of security compliance posture, verification of legal authorizations and controls.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

Essential Security Training Controls

A. INTRODUCTION

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

2. This Security Training framework applies to all employees, management, and relevant stakeholders of the organization. It establishes mandatory information security awareness, specialized role-based training, and continuous education requirements to ensure secure practices across all levels. The framework covers training design, delivery, documentation, and evaluation, ensuring compliance with regulatory obligations, alignment with risk management objectives, and adaptation to evolving threats and technologies.

B. SECURITY TRAINING CONTROLS

3. The organization shall establish and maintain a structured information security training program that defines priorities, topics, schedules, resources, delivery methods, and target audiences to ensure comprehensive coverage and program effectiveness aligned with organizational objectives and recommendations from NTISB, nCERT and sector regulator.

4. All employees and users shall complete mandatory information security awareness sessions before being granted system access, with annual refreshers and ad-hoc sessions conducted to address emerging threats, incidents, or regulatory changes.

5. Employees working in information security and IT shall receive role-specific training and obtain relevant certifications in information security and IT service management.

6. All personnel in high-risk or privileged roles (such as IT administrators, developers, incident responders, and forensic analysts etc.) shall complete specialized role-based security training, in addition to baseline awareness programs, as a condition for being granted system or data access.

7. Specialized training requirements shall be identified through risk assessments, audits, incidents, and regulatory obligations, and shall be refreshed periodically, at least annually.

8. Information Security training and awareness sessions shall address key areas, including but not limited to, password management, phishing, social engineering, secure remote work, mobile device security, data privacy, and incident reporting. These trainings and awareness sessions shall be delivered through multiple formats (e.g. e-learning, instructor-led sessions, webinars, tabletop exercises), with content reviewed and updated regularly.

9. All training participation shall be documented capturing attendee details, training dates, module names, and assessment outcomes, with records securely stored, backed up, and retained in accordance with regulatory and organizational requirements, and made available for audits or compliance checks.

10. The organization shall evaluate the effectiveness of its information security training and awareness program regularly through simulations, assessments, and performance monitoring, ensuring that outcomes directly update corrective and preventive actions.

11. The organization shall continuously strengthen its training and awareness program by incorporating feedback from employees, audits, and incident reviews, ensuring alignment with evolving threats and organizational needs.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential System and Communication Protection Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework: **"Essential System and Communication Protection Controls"**, outlines the baseline of information security system and communication protection controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all organizational systems, networks, communication channels, and supporting technologies used to collect, transmit, process, or store information. It covers employees, third parties, and any other entities with access to organizational systems, ensuring secure design, implementation, and management of communication and system protections across the enterprise.

B. NETWORKS SECURITY

3. The organization shall establish, document, and formally approve network security requirements and ensure that approved security controls, in line with defense-in-depth principles and the organization's risk management strategy, are implemented and maintained to protect organizational networks.

4. The information security requirements for network security management shall include at least the following: -

a) Physical protection of all network infrastructure and information assets.

b) Appropriate segregation of networks across different environments and functions.

c) Appropriate perimeter security controls (like Firewall, IDS/IPS, etc. as per the requirements identified by the steering committee of information security).

d) Remote connectivity (on strict need basis) secured with appropriate measures, including VPNs, monitoring, auditing, and preferably multi-factor authentication.

e) Secure management of wireless networks, isolated from critical internal resources.

f) Systems with internet access are logically or physically segregated from critical information systems.

g) Network activity is logged and monitored to support incident investigation, security auditing, and compliance requirements

h) Establish and enforce change management and configuration management controls for all network changes and configuration updates.

C. PROTECTION OF ENDPOINT COMPUTING DEVICES

5. Information security requirements for protecting endpoint computing devices (Servers, workstations, desktops, laptops, mobile phones, tablets, etc.) shall be defined, documented, approved and implemented.

6. The information security requirements for protecting endpoint computing devices shall include at least the following:

a) Appropriate security solutions (anti-virus, anti-malware, EDR, XDR, etc.) depending upon the classification of asset and architecture of the organization. Endpoints shall not be left without any appropriate protection.

b) Establish and enforce controls governing the secure use of external or removable storage media to protect organizational information assets.

c) Maintain up-to-date endpoint computing devices through regular patch management and updates.

D. EVENT LOGS AND MONITORING

7. Information security requirements for event logs and monitoring shall be defined, documented, approved and implemented.

8. Event log and monitoring requirements shall include at least the following: -

a) Comprehensive event logging of, at a minimum, all critical assets, remote access connections and privileged user accounts.

b) Centralized log management and monitoring to aggregate, correlate, and continuously analyze cybersecurity events.

c) Retention of critical event logs for a minimum of 12 months for critical assets and for non-critical assets that impact critical assets; and for a minimum of 3 months for all other assets.

d) Systems synchronized clocks using NTP (Network Time Protocol).

e) Protection of active and archived logs from unauthorized tampering, destruction, or alteration, whether intentional or unintentional, to ensure their integrity and accuracy.

E. BACKUP AND RECOVERY MANAGEMENT

9. The organization shall ensure that information security requirements for backup and recovery management are formally defined, approved, documented, and implemented.

10. The organization shall define and approve recovery parameters, including recovery point objectives (RPO) and recovery time objectives (RTO), and ensure that backup and recovery arrangements for critical technology and information assets are designed, implemented, and periodically tested to meet these objectives.

11. The organization shall ensure that backup media, storage and facility are adequately secured and protected. Organization should perform risk assessment of the backup and restore process; and define, implement and document appropriate controls.

12. Regularly testing the restoration process should be conducted in line with the defined RTO/RPO. The integrity checks should be performed for assurance purpose.

13. The organization should devise a mechanism for continuous monitoring and evaluation of backup/restore activities. Regular audits should include this process for better visibility of effectiveness of this process to the senior management.

F. VULNERABILITY AND PATCH MANAGEMENT

14. Vulnerabilities and patch management life cycle shall be defined, documented, approved and implemented.

15. Vulnerability management shall include regular vulnerability assessments, classification of vulnerabilities based on criticality level, and effective patch management.

16. The organization shall implement a comprehensive patch management program including vulnerability testing before deployment, continuous monitoring, and a defined rollback strategy.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Identity and Access Management Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework: **"Essential Identity and Access Management (IAM) Controls"**, outlines the baseline of information security identity and access management controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework governs the management of all users, services, systems, and privileged accounts across the organization's technology resources. It covers on-premises, cloud, and third-party environments, including processes for identity governance, lifecycle management, authentication, credential management, and authorization.

B. IDENTITY AND ACCESS MANAGEMENT

3. The organization shall define, document, approve, and implement identity and access governance processes to ensure accountability, compliance, and secure management of all identities.

4. The organization shall establish and enforce lifecycle processes for the creation, maintenance, and timely deprovisioning of user, service, and system accounts.

5. The organization shall enforce authentication framework with strong passwords, multi-factor and adaptive methods, supported by session management, monitoring, and standardized tools to ensure secure access aligned with system sensitivity and risk.

6. The organization shall enforce secure credential lifecycle management process, including generation, storage, distribution, rotation, review, revocation, and disposal.

7. The organization shall ensure that user access rights are regularly reviewed and are promptly modified or revoked upon role change, transfer, or termination.

8. The organization shall enforce the principle of least privilege through defined access control models, ensuring that all access to systems and data is authorized strictly based on documented business need and formally approved.

9. The organization shall centrally manage all official social media accounts through clearly defined ownership, role-based access controls, and formal content approval processes.

C. PRIVILEGED ACCESS MANAGEMENT

10. The organization shall classify privileged accounts based on business impact and enforce strict governance through approval workflows, dedicated non-shared access, secure vaults, just-in-time elevation, and continuous session monitoring.

11. The organization shall ensure that emergency (break-glass) and third-party privileged access is granted only with enhanced authorization, is limited in duration, and is fully auditable, with privileged activities logged and monitored.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Data Protection and Privacy Controls

NTISB

A. INTRODUCTION

1. "Pakistan Information Security Framework: **"Essential Data Protection and Privacy Controls"**, outlines the baseline of information security data protection and privacy controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all employees, contractors, consultants, third-party service providers, and any other individuals or entities that process or access the organization's data. It covers all forms of data, including electronic, paper-based, structured, and unstructured information, regardless of where it is stored or processed. It also applies to all business functions, systems, applications, networks, and processes that involve personal, sensitive, or confidential data, whether processed within the organization's premises, in cloud environments, or through third-party arrangements.

B. DATA PRIVACY

3. The organization shall establish and maintain a clear privacy governance structure with defined roles, responsibilities, and accountability for data protection.

4. The organization shall collect and process personal data only where a lawful basis exists under applicable data protection laws, including consent where required. Privacy notices, wherever applicable, shall clearly inform data subjects of the purpose, legal basis, and use of their personal data.

5. Privacy Impact Assessments shall be conducted for new systems, projects, or processes to identify and mitigate potential privacy risks.

6. Organization shall develop and implement data privacy policy while keeping the principles of purpose limitation, data minimization, accuracy, storage limitation, maintaining confidentiality, integrity and accountability.

7. The organization shall ensure that access to personal data is monitored, logged, and auditable.

8. Organizations shall establish and maintain a documented data retention schedule. An illustrative retention schedule template is provided in Table 1, as an example, to support consistent classification, retention, and disposal of data in accordance with legal, regulatory, and business requirements.

Table 1: Data Retention Schedule Table (Example)

Data Category	**Data Description**	**Data Owner**	**Legal/ Regulatory Basis**	**Retention Trigger**	**Retention Period**	**Storage Location**	**Disposal Method**
Personal Data	Employee Record	To be defined	To be defined	End of employment	To be defined	HR system	Secure deletion
Financial Data				Fiscal year closure			
Operational Data				Creation date			
Customers data				End of contract			

C. DATA SECURITY

9. All organizational data shall be classified according to sensitivity, criticality, and regulatory requirements to ensure appropriate protection.

10. Personal and organizational data shall be handled, transmitted, and stored only in accordance with defined security procedures and legal requirements.

11. Access to data shall be granted strictly on the principle of least privilege and role-based access, with regular reviews and monitoring.

12. Data classified as critical or highly critical with respect to confidentiality, where the unauthorized disclosure could cause catastrophic or serious impact, shall be encrypted during transmission and preferably during storage.

13. The organization shall implement measures to maintain the accuracy, completeness, and consistency of data throughout its lifecycle.

14. Data shall be retained only for as long as necessary to fulfill business or legal purposes and shall be securely and permanently disposed of when no longer required.

15. Data shall be regularly backed up and recovery mechanisms shall be tested to ensure business continuity, in case of data loss, based on the classification of data.

16. Data access, processing, and security events shall be continuously monitored and logged to detect, prevent, and investigate unauthorized activities.

D. DATA BREACH

17. All systems and networks shall be continuously monitored to detect potential data breaches or anomalous activities at the earliest possible stage.

18. Upon detection of a breach, immediate containment measures shall be applied to limit impact and prevent further compromise.

19. The organization shall ensure timely reporting of data breaches (72 hours for critical infrastructure and 120 hours for non-critical infrastructure) to concerned regulator and nCERT.

20. Appropriate policy and procedure should be preferably developed to notify affected individuals of the breaches about compromise of their personal data, including details of risks and recommended protective measures.

21. When required, public statements regarding breaches should be issued in a controlled and coordinated manner to ensure accuracy and maintain trust.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Incident Response Controls

NTISB

A. INTRODUCTION

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

2. This framework applies to all organizational functions, systems, and processes involving sensitive data, across all internal and external environments. It establishes the foundation of preparing for, responding to, and recovering from security incidents and disruptions to protect national digital assets, organizational resilience, and public trust.

B. INCIDENT MANAGEMENT

3. The organization shall formulate cyber security incident management policy and procedure for the preparation, detection, response, mitigation, reporting, recovery, remediation and lessons learned.

4. The organization shall maintain classification of information security incidents based on severity and impact.

5. The organization shall manage incidents using an approved incident response framework that assigns clear ownership and accountability and ensures consistent handling across the incident lifecycle.

6. Organizations, other than service providers, shall perform a requirement analysis and feasibility assessment to determine the establishment of a Security Operations Center (SOC) and/or the acquisition of SIEM or other relevant security monitoring solutions.

7. The organization shall maintain incident readiness through clear policies, adequate resources, and skilled teams. Regular mock drills shall be performed which will help to identify any loopholes in the whole process, gradually improve readiness capabilities, improve visibility of the activities performed and enhance confidence of senior management.

8. The organization shall establish incident response roles and responsibilities, along with the corresponding authority and dependency levels.

9. The organization shall report information security incidents as follows:

a) Critical infrastructure incidents: Initial reporting to sectoral regulators/CERTs and nCERT upon verification of incident, followed by detailed reporting within 72 hours.

b) All verified incidents for non-critical infrastructure shall be reported to sectoral regulators/CERTs within 120 hours.

10. The organization shall document incident lessons learned for each security incident and implement corrective actions within defined timelines to prevent recurrence.

C. BUSINESS CONTINUITY PLAN (BCP) (APPLICABLITY TO BE ASSESSED BY RELEVANT INFORMATION SECURITY STEERING COMMITTEE)

11. The Business Continuity Program shall be governed by appropriate entity designated by information security steering committee, with each department nominating a Continuity Focal Person to maintain plans and coordinate response efforts.

12. Based on an annual Business Impact Analysis (BIA), that categorizes critical functions and their interdependencies, the organization shall

develop, approve, and implement a comprehensive business continuity plan addressing tiered recovery, backup or alternate sites, remote work arrangements, and supply chain resilience.

13. 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.
14. Invocation of BCP must follow documented procedure for damage assessment, communications, recovery and restoration, with all activities logged.
15. The organization shall conduct annual simulations or exercises to test recovery capabilities, ensure compliance and build resilience with all tests evaluated against defined success criteria.

D. DISASTER RECOVERY PLAN (APPLICABLITY TO BE ASSESSED BY RELEVANT INFORMATION SECURITY STEERING COMMITTEE)

16. The Disaster Recovery Plan (DRP) shall be activated by the organization upon defined triggers like RTO and RPO.
17. Structured communication during a DR event shall be delivered to all stakeholders using formats and escalation routes aligned with the incident management and response plan, and all activities must be documented.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Physical Security Controls

NTISB

A. INTRODUCTION

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

2. This framework applies to all organizational systems, networks, communication channels, and supporting technologies used to transmit, process, or store information. It covers employees, consultants, contractors, third parties, and any other entities with access to organizational systems, ensuring physical security of digital assets across the enterprise.

B. PHYSICAL SECURITY CONTROLS

3. Organizations shall define, document, approve, and implement information security requirements for the physical protection of information and technology assets.

4. The information security requirements for physical protection of information and technology assets shall include at least the following:

a) Authorized access to sensitive areas and assets within the organization (e.g., data center, sensitive information processing facilities, security surveillance center, network cabinets, etc.).

b) Appropriate access control mechanism for different areas and facilities (e.g. biometric locks, smart cards, keypads, manned guards, etc.).

c) Surveillance systems where required (e.g. CCTV cameras, motion sensors, extra lighting, etc.).

d) Perimeter protection as per requirement (e.g. fencing on boundary wall, bollards, special purpose gates, etc.).

e) Implement robust facility access controls, monitoring, and surveillance, including entry/exit records, with secure storage and protection of access records.

f) Secure destruction and re-use of physical assets that hold classified information (including documents and storage media)

5. The organization shall establish controls to ensure that storage media used for Confidential or Secret information is removed or securely handled before devices are sent outside organization for repair.

6. Fire safety and protection mechanism should be in place. The organization shall ensure that appropriate controls are in place against fire eruption and all the employees are adequately trained to respond under any fire incident.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Supply Chain Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework: **"Essential Supply Chain Controls"**, outlines the essentials of information security supply chain risk management controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all suppliers, subcontractors, and third parties that provide goods, services, or data to the organization. It covers the entire supplier lifecycle, including identification, onboarding, monitoring, compliance, incident management, off boarding, and associated supply chain risk management activities. The scope extends to subcontractors and fourth parties where they interact with organizational systems, services, or data.

B. SUPPLY CHAIN CONTROLS

3. The organizations shall define, document, approve and implement policies, procedures, and processes for managing supply chain risks for products, systems, and services provided by third parties.

4. The organization shall identify, assess and classify supply chain risks across defined categories with special emphasis on information security, third-party access, operational dependency and critical supplier dependencies.

5. The organization shall implement risk-specific mitigation strategies, including supplier diversification, contingency planning, contractual controls, information security audits, and business continuity measures, to reduce supply chain risks to acceptable levels.

6. All identified supply chain risks shall be continuously monitored, tracked, and reviewed at defined intervals or upon significant changes, to ensure timely response, escalation and remediation.

7. Organizations procuring services like cloud services, Data Centers, Web hosting, Secure software development, etc. must ensure that the service providers comply with relevant policy frameworks in the PISF and/or applicable laws, regulations and sector specific policies

8. All suppliers must be identified, documented, and classified based on the criticality of products, services, systems and data they provide to the organization.

9. The organization shall conduct risk-based due diligence on all suppliers prior to engagement to ensure compliance with applicable security, legal, and regulatory requirements.

10. All supplier agreements and Service Level Agreements (SLAs) shall include contractual provisions covering information security, data protection, confidentiality, audit rights, incident notification timelines, and compliance obligations.

11. The organization shall be accountable for all the risk accepted by any third party, which can have significant impact on the organization.

12. The organization shall ensure transparency and verification of supplier source, including the origin, authenticity and integrity of products, services, software components, and data.

13. Organizations shall ensure that suppliers handle, process, store, and share organizational data strictly in accordance with approved security and privacy requirements (Ref: Data protection and privacy policy).

14. The organization shall monitor supplier compliance through defined KPIs, periodic reviews, risk assessments, and continuous oversight of cybersecurity.

15. Organizations shall ensure that suppliers detect, report, and coordinate with the organization on security incidents affecting data or services, in accordance with defined procedures, notification timelines, and joint incident response mechanisms.

16. Organizations shall ensure that suppliers maintain documented and tested business continuity and disaster recovery capabilities appropriate to ensure resilience of critical services.

17. Organizations shall ensure that the suppliers remain fully accountable for the actions of their subcontractors and fourth parties.

18. Organizations shall ensure secure off-boarding of supplier, including returning or securely destroying data, revoking access, undergoing exit audits, and ensuring service continuity and data integrity upon contract completion/ Termination.

19. Significant changes in supplier scope, ownership, location, or service delivery shall trigger a reassessment of supply chain risks.

20. The organization shall identify and manage concentration risks arising from single-source or highly dependent suppliers.

21. Relevant personnel involved in procurement and supplier management shall receive periodic training on supply chain risk management requirements.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

Essential Audit Controls

NTISB

A. INTRODUCTION

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

2. This framework defines the organization's framework for internal and external information security audits, in alignment with regulatory requirements and organizational objectives. Aim is to strengthen governance through independent information security audits and continuous improvement.

B. INFORMATION SECURITY AUDIT

3. The organization shall establish an independent internal audit function responsible for information security audits, with audits conducted at least annually. While the oversight/external audits may be conducted by the relevant regulator and nCERT/NTISB as applicable.

4. The organization shall develop and adopt a Control Self-Assessment (CSA) process to transform the audit function from a reactive, periodic compliance check to a proactive, continuous, and integrated risk management process.

5. The organization shall mandate that all internal and external information security audits are conducted by independent, certified, and qualified auditors, selected through formally defined criteria.

6. Audit firms, registered with nCERT/ sectoral CERTs/ relevant regulator, should be preferably engaged for consultancy, internal audits and external audits as per the criteria.

7. The organization shall enforce confidentiality obligations, including Non-disclosure agreements (NDAs), least-privilege access controls, and apply technical safeguards such as data masking or watermarking, acknowledging audit data sensitivity.

8. The organization shall initiate information security audits on a risk-driven basis, aligned with organization risk register, regulatory obligations, executive directives, and significant security incidents, ensuring that audit scope directly reflects business priorities and threat landscapes.

9. The organization shall require every information security audit to be supported by a documented and approved audit plan, aligned with recognized standards, defining scope, objectives, tools, timelines, and resource allocation.

10. The organization shall provide all mandatory documentation to the assigned auditor, including but not limited to the control Applicability statement, Risk Treatment Plan and the duly approved scope of the audit, signed by the competent authority. These documents shall be accurate, complete and up to date.

11. The organization shall ensure that all audit findings are supported by verifiable, sufficient, and securely stored evidence, collected and retained through standardized processes that ensure integrity, traceability and accountability.

12. The organization shall ensure that audit results are documented in a standardized report format, communicated to relevant stakeholders, and retained in compliance with regulatory requirements and organizational policies.

13. The organization shall enforce a formal closure and follow-up process for each audit, including confirmation of completed corrective actions, validation of remediation effectiveness, documented risk acceptance where applicable, escalation of overdue actions, documentation of lessons learned, and integration of findings into organizational risk management practices.

14. The organization shall establish a process of periodic review and continuous improvement for its audit framework, ensuring alignment with evolving information security standards, regulatory changes, organizational objectives, and emerging threat landscapes.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Data Center and Web Hosting Services Controls

NTISB

A. INTRODUCTION

Pakistan Information Security Framework: **"Essential Data Center and Web Hosting Services Controls"**, outlines the baseline of information security data center controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

This framework applies to data centers, email and all hosting services, encompassing physical infrastructure, IT systems, and communication platforms used to store, process, or transmit data.

B. DATA CENTER

1. The data center's security framework shall implement comprehensive physical controls, including but not limited to controlled physical access, perimeter protection, video surveillance, visitor management, and other necessary safeguards.

2. Organizations that provide hosting services to other entities, or that maintain their own data centers or servers, shall implement and maintain the following minimum security controls:

   a) Implement network and perimeter security controls, including Next generation firewalls (NGFWs), WAFs, IDS/IPS, DDoS protection, DLP solutions, network segmentation, DMZs, and use of secure communication protocols.

   b) Implement server hardening practices including limiting unnecessary services, disabling unused ports, enforcement of secure configuration, configuration baseline management and enforcing secure protocols.

   c) Implement and maintain a documented patch and vulnerability management process to identify, prioritize, remediate, and track vulnerabilities, supported by regular vulnerability assessments and remediation verification.

d) Develop, implement, and regularly test Business Continuity and Disaster Recovery Plans to ensure operational continuity in line with organizational requirements, recovery objectives and service criticality.

e) Deploy continuous monitoring and incident response solutions, including SIEM, SOAR, and SOC.

f) Implement structured cable management practices, including labelling, separation of power and data cables, and regular inspections to prevent operational and security risks.

g) Secure logging and monitoring practices, including retention of critical security event logs for a minimum of 12 months, ensuring integrity, availability, and audit traceability.

h) Secure backup and recovery mechanisms, including encryption, access controls, periodic restoration testing, and offsite or geographically separate backup storage.

3. Data centers shall undergo regular internal audits and at least one independent annual third-party audit, covering physical, technical, and operational security controls.

4. Organizations that are unable to meet the defined audit and compliance requirements shall ensure migration of services to a secure and compliant data center that meets the requirements of this framework and applicable regulatory obligations.

5. All data centers shall strictly comply with all relevant and applicable security requirements defined in the nCERT Essential Framework, including Asset and Risk Management, System and Communication Protection, Data Protection, Identity and Access

Management, Incident Response and audit. Compliance with these requirements shall be mandatory and subject to verification and audit.

C. EMAIL AND WEB HOSTING SERVICES

6. Organizations providing email and hosting services to other government organizations or maintaining email or any other hosting services for their own users, shall define, document, approve, and implement information security requirements to ensure the confidentiality, integrity and availability of the hosted services.

7. The information security requirements for the email service shall include at the least the following:

a) Advanced email threat protection controls to detect and block phishing, malware, spam, and malicious content.

b) Implement multi-factor authentication for administrative, remote and webmail access.

c) Ensure email archiving, backup and restoration capabilities to support operational continuity and regulatory compliance.

d) Monitoring, detection, and response mechanisms to protect against Advanced Persistent Threats (APTs) and targeted attacks.

e) Email domain validation and authentication controls, including Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting and Conformance (DMARC) or equivalent measures.

D. WEB APPLICATION SECURITY

8. Organizations shall define, document, approve, and implement information security requirements for all internal and externally accessible web applications, regardless of the hosting environment (on-premises, in the cloud or third-party service providers)

9. The information security requirements for web applications shall include at least the following:

a) Controls to prevent unauthorized access, abuse and malicious activity.

b) Secure architectural and design principles with defense-in-depth protection.

c) Secure communication protocols for data in transit.

d) Well-defined secure usage practices and user awareness controls.

e) Regular vulnerability assessments, penetration testing, and remediation tracking.

f) Maintenance of applications using up-to-date, supported and securely configured components.

g) Strong authentication and session management mechanisms.

h) Secure software development lifecycle (SSDLC) practices, including code reviewing, security testing, and approval prior to deployment.

10. Organizations hosting their websites and applications outside Pakistan shall plan migration to data centers within Pakistan's geographical boundaries.

11. Organizations shall remain accountable to ensure that requisite security requirements are clearly defined, implemented, and monitored through contracts, Service Level Agreements (SLAs), and right-to-audit clauses with developers, hosting providers and cloud service providers.

E. ENVIRONMENTAL CONTROLS (DATA CENTERS AND HOSTING FACILITIES)

12. The organization shall implement and maintain environmental controls to protect data center facilities, systems, and equipment from environmental threats that may impact availability, integrity, or safety of operations.

13. Data centers shall be equipped with power supply resilience mechanisms, including uninterruptible power supplies (UPS), backup generators, and redundant power distribution, sufficient to meet defined availability and recovery requirements.

14. The organization shall implement environmental monitoring systems to continuously monitor temperature, humidity, power stability, and other critical environmental parameters, with automated alerts and defined response procedures for threshold breaches.

15. Data centers shall implement heating, ventilation, and air conditioning (HVAC) controls designed to maintain environmental conditions within manufacturer-recommended operating ranges and to prevent overheating, condensation, or equipment degradation.

16. The organization shall deploy fire detection and suppression systems appropriate for data center environments, including early warning smoke detection, automatic fire suppression, and safe evacuation mechanisms, with regular inspection, testing, and maintenance.

17. Data centers shall implement controls to mitigate risks from water leakage, flooding, dust, vibration, and other physical or environmental hazards, including raised flooring, leak detection systems, and appropriate facility design.

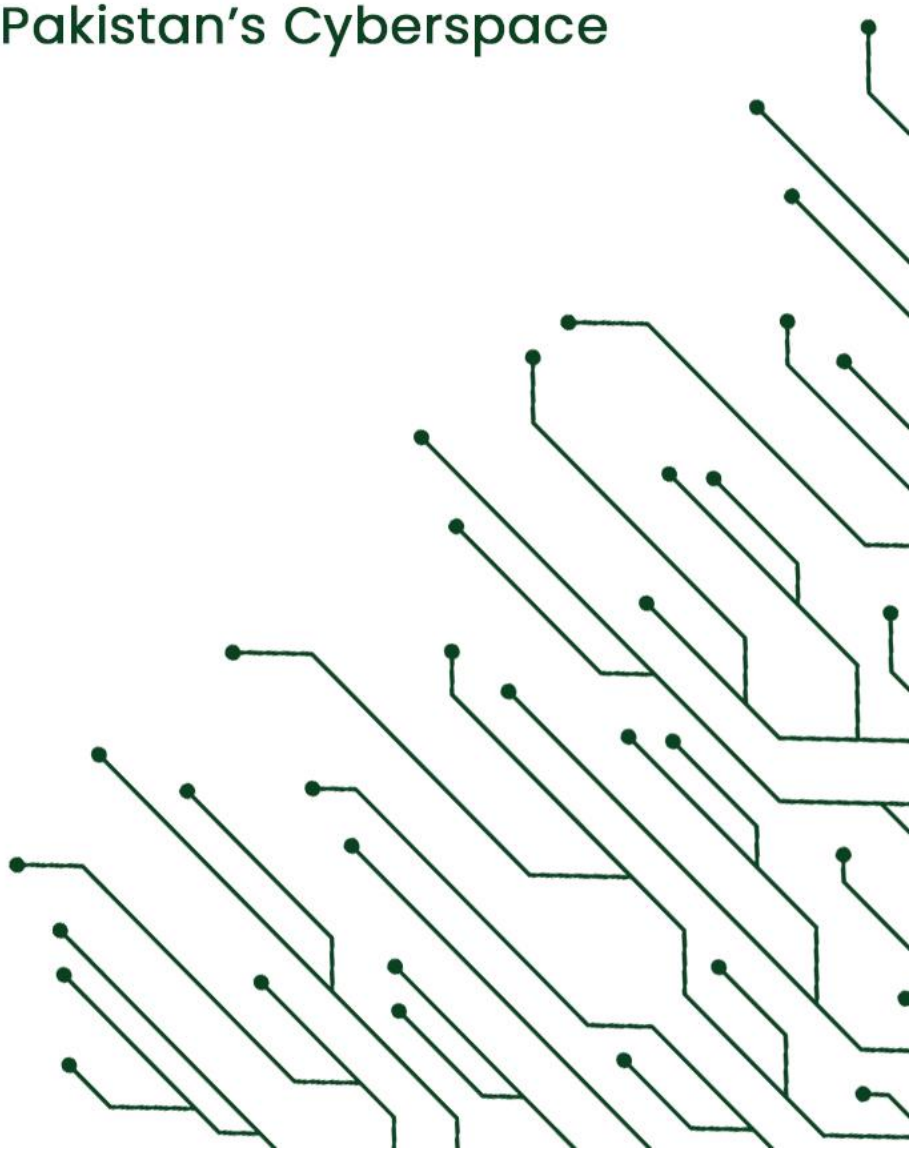
18. The organization shall document and maintain environmental control procedures, including preventive maintenance schedules, escalation processes, incident response actions, and roles and responsibilities for facility management personnel.

19. Environmental control systems and safeguards shall be periodically tested, inspected, and audited to verify effectiveness, reliability, and compliance with regulatory, contractual, and organizational requirements.

20. The organization shall ensure that environmental incidents or control failures affecting data center operations are logged, investigated, reported to relevant stakeholders, regulators, and incorporated into risk management and continuous improvement processes.

PKCERT

Safeguarding Pakistan's Cyberspace



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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

ESSENTIAL SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC) CONTROLS

NTISB

A. INTRODUCTION

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

2. This framework applies to all individuals and entities involved in the development, acquisition, deployment, and maintenance of software and applications. It covers all types of applications and environments, ensuring that security controls are systematically integrated throughout every phase of the software life cycle to protect personal, sensitive, and business-critical data in compliance with national cybersecurity and information security regulations and standards.

B. SSDLC CONTROLS

3. All those organizations involved in software development for other organizations or for internal use shall ensure that requirements for SSDLC shall be defined, documented, approved and implemented.

4. The requirements for SSDLC shall have but not limited to the following:

a) Embed security from the earliest stages of software development and ensure alignment with recognized secure development standards and frameworks.

b) Security integrated throughout all phases of the SDLC, including requirements analysis, architecture and design, threat modeling, development, testing, deployment, and maintenance, incorporating risk, compliance and regulatory consideration.

c) Security validation and approval of code before release, with post-implementation reviews.

d) Appropriate role based training for developers and evaluators in secure coding practices, secure design principles, and emerging threats relevant to the technologies in use.

e) Separate development, testing, and production environments with controlled access, change management, and monitoring.

f) Maintain secure repositories for source code, build artifacts and configuration items.

g) Security review and approval for all commercial, open-source, and third-party components (software libraries, modules, middleware, etc.) before acquisition and integration.

h) Adoption of approved tools for code scanning, security testing, dependency management, and version control, integrated into the CI/CD pipeline.

i) Comprehensive testing through expert code reviews and manual/automated assessments of all software and applications (e.g., SAST, DAST, IAST, SCA), appropriate to the application's risk and criticality.

j) Ensure that independent or third-party security testing is performed for critical software and applications as part of the secure development and acquisition lifecycle.

PKCERT

Safeguarding Pakistan's Cyberspace

info@pkcert.gov.pk

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

Safeguarding Pakistan's Cyberspace

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