PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

Muhammad Mehtab Abdullah
Director Office (IT)
14 October 2026 03:22:13 PM

Table of Contents

1 Introduction 9

1.1 Applicability 9

1.2 PISF Implementation Road Map 10

1.3 Compliance Criteria 11

2 Essential Governance Controls 14

2.1 Introduction 14

2.2 PISF Implementation Ecosystem 14

2.3 Organizational Structure 14

2.4 Policies and Procedures 16

2.5 Leadership and commitment 16

2.6 Change Management 17

2.7 Compliance and Third-Party Management 17

3 Essential Asset and Risk Management Controls 18

3.1 Introduction 18

3.2 Asset management 18

3.3 Software and License Management 20

3.4 System Categorization and Classification 21

3.5 Risk Management 24

4 Essential Security Training Controls 26

4.1 Introduction 26

4.2 Security Training Controls 26

5 Essential System and Communication Protection Controls 28

5.1 Introduction 28

5.2 Networks Security 28

5.3 Protection of Endpoint computing devices 29

5.4 Event Logs and Monitoring 29

5.5 Backup and Recovery Management 30

5.6 Vulnerability and Patch Management 30

6 Essential Identity and Access Management Controls 31

6.1 Introduction 31

PKCERT

6.2 Identity and Access Management 31
6.3 Privileged Access Management 32
7 Essential Data Protection and Privacy Controls 33
7.1 Introduction 33
7.2 Data Privacy 33
7.3 Data Security 34
7.4 Data breach 35
8 Essential Incident Response Controls 36
8.1 Introduction 36
8.2 Incident management 36
8.3 Business Continuity Plan (BCP) (Applicability To Be Assessed By Relevant Information Security Steering Committee) 37
8.4 Disaster Recovery Plan (Applicability To Be Assessed By Relevant Information Security Steering Committee) 38
9 Essential Physical Security Controls 39
9.1 Introduction 39
9.2 Physical Security Controls 39
10 Essential Data Centre and Web Hosting Services Controls 41
10.1 Introduction 41
10.2 Data Center 41
10.3 Email and Web Hosting Services 42
10.4 Web Application Security 43
10.5 Environmental Controls (Data Centers and Hosting Facilities) 44
11 Essential Secure Software Development Life Cycle Controls 46
11.1 Introduction 46
11.2 SSDLC Controls 46
12 Essential Supply Chain Management Controls 48
12.1 Introduction 48
12.2 Supply chain controls 48
13 Essential Audit Controls 51
13.1 Introduction 51
13.2 Information Security Audit 51
14 Essential CII Protection Controls 53

PKCERT

14.1 Introduction 53
14.2 Governance & Resource Allocation 53
14.3 Critical Asset Classification Framework 55
14.4 CIA-Aligned Control Implementation 57
Annex-A PISF CONTROLS 60

Muhammad Usman Abdullah
Sr. Director (Cert)
16 October 2026 03:25:03 PM
PKCERT

List of Tables

Table 1.1: In scope and Out of Scope Detail 12
Table 1.2: Compliance Criteria 13
Table 3.1: Asset Register 19
Table 3.2: Classification Scheme 21
Table 3.3: Classification mapping with Impact on CIA 21
Table 3.4: Classification Scheme 23
Table 3.5: Attributes for Risk Register 25
Table 7.1: Data Retention Schedule Table (Example) 34
Table 14.1: Classification Scheme 55
Table 14.2: Classification mapping with Impact on CIA 55

List of Figure

Figure 1.1: Implementation Road Map 11

Muhammad Hussein Abdullah
Sr. Director (CERT)
16 October 2026 03:22:41 PM
PKCERT

ACRONYMS

ABBREVIATION	TERM
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BS-20	Basic Scale 20
CERT	Cyber Emergency Response Team
CERTs	Cyber Emergency Response Teams
CIA	Confidentiality, Integrity, and Availability
CII	Critical Information Infrastructure
CIIs	Critical Information Infrastructures
CIIO	Critical Information Infrastructure Owner
CIIP	Critical Information Infrastructure Protection
CI/CD	Continuous Integration / Continuous Deployment
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CCTV	Closed-Circuit Television
CRO	Chief Risk Officer
CSA	Control Self-Assessment
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMZ	Demilitarized Zone
DMZs	Demilitarized Zones
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EDR	Endpoint Detection and Response
HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning

Muhammad Abdullah Ashraf Abdullah
Director Officer
14 October 2026 03:03:03 PM
PKCERT

IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IPS	Intrusion Prevention System
IRP	Incident Response Plan
ISMS	Information Security Management System
IT	Information Technology
IT/ICT	Information Technology / Information and Communication Technology
KPI	Key Performance Indicator
KPIs	Key Performance Indicators
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair / Mean Time to Response
NDA	Non-Disclosure Agreement
NDAs	Non-Disclosure Agreements
NGFW	Next Generation Firewall
NGFWs	Next Generation Firewalls
nCERT	National Cyber Emergency Response Team
NTISB	National Telecom and Information Security Board
NTP	Network Time Protocol
PII	Personally Identifiable Information
PISF	Pakistan Information Security Framework
PKCERT	Pakistan Cyber Emergency Response Team
PPRA	Public Procurement Regulatory Authority
PSS	Pakistan Security Standard
RACI	Responsible, Accountable, Consulted, and Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective

PKCERT

RTO/RPO	Recovery Time Objective / Recovery Point Objective
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLAs	Service Level Agreements
SOC	Security Operations Center
SOAR	Security Orchestration, Automation, and Response
SOP	Standard Operating Procedure
SOPs	Standard Operating Procedures
SPF	Sender Policy Framework
SPOF	Single Point of Failure
SPOFs	Single Points of Failure
SSDLC	Secure Software Development Life Cycle
UPS	Uninterruptible Power Supply
WAF	Web Application Firewall
WAFs	Web Application Firewalls
XDR	Extended Detection and Response

Muhammad Jalal Aftab Ullah
Digital Signature
16 October 2026 03:22:03 PM
PKCERT

1 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 domains:

i). Essential Governance Controls
ii). Essential Asset and Risk Management Controls
iii). Essential Security Training Controls
iv). Essential System and Communication Protection Controls
v). Essential Identity and Access Management Controls
vi). Essential Data Protection and Privacy Controls
vii). Essential Incident Response Controls
viii). Essential Physical Security Controls
ix). Essential Data Centre and Web Hosting Services Controls
x). Essential Secure Software Development Life Cycle Controls
xi). Essential Supply Chain Management Controls
xii). Essential Audit Controls
xiii). Essential CII Protection Controls

1.1 Applicability

3. This framework shall be applicable to all Federal and Provincial Government Ministries, Divisions and Departments, autonomous bodies, corporations, CERTs and 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.

PKCERT

1.2 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.

PKCERT

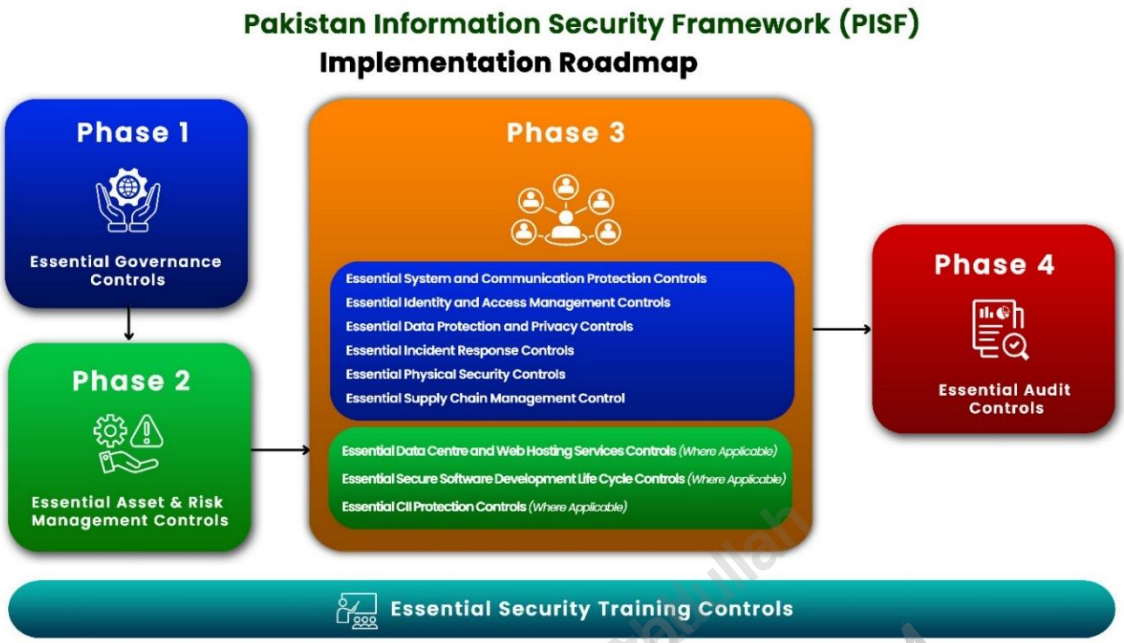

Figure 1.1: Implementation Road Map

1.3 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 1.1 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.

PKCERT

Table 1.1: 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 1.2 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 attached as Annex-A of this Framework.

PKCERT

Table 1.2: 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.

Muhammad Usman Atta Ullah
Security Officer (IT)
14 October 2026 03:25:43 PM
PKCERT

2 ESSENTIAL GOVERNANCE CONTROLS

2.1 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.

2.2 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.

2.3 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.

Muhammad Usman Abdullah
Sr. Director (CERT)
16 October 2026 03:08:43 PM
PKCERT

8. A dedicated 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 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.

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 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 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 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 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.

PKCERT

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

2.4 Policies and Procedures

19. The 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 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.

2.5 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 information security teams in establishing a resilient security posture that aligns with the organization's risk profile and sensitivity levels.

Muhammad Ubaid Ullah Afzal Ullah
Director Office
16 October 2026 03:02:43 PM
PKCERT

2.6 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 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.

2.7 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.

MuhammadIshmaKhalilah
Section Officer
16 October 2026 03:23:13 PM
PKCERT

3 ESSENTIAL ASSET AND RISK MANAGEMENT CONTROLS

3.1 Introduction

1. Pakistan Information Security Framework: **"Essential Asset and Risk Management Controls"**, outlines the baseline of information security asset & risk management controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This document defines the organization's framework for managing assets, software, systems, risks, and information security audits. It applies to all organizational assets, personnel, and processes, ensuring effective asset lifecycle management, software license compliance, system classification and decommissioning as well as structured risk assessment and treatment.

3. An **information asset** refers to information and data, whether in electronic or physical form, that is owned, managed, or processed by the organization, carries value to the organization, and consequently necessitates protecting against unauthorized access, disclosure, modification, or destruction.

4. A **technology asset** is any hardware, software, system, network component, or technical infrastructure that is used to collect, store, process, transmit, or protect information and therefore requires security controls to preserve confidentiality, integrity, and availability.

3.2 Asset management

5. All information and technology assets shall be formally identified, classified, and documented in the Asset Register, ensuring complete and accurate recording at the time of acquisition, throughout the lifecycle of the asset.

6. The organization shall designate asset ownership and document in the Asset Register. Asset owner shall be accountable for ensuring that information assets are appropriately classified, protected, and used in accordance with organizational requirements, risk appetite, and applicable legal and regulatory obligations.

Muhammad Ahsan Abdullah
Director/Officer
14 October 2026 03:25:41 PM
PKCERT

7. Essential metadata attributes for each asset shall be recorded, including asset name or unique identifier, asset type with description, serial number, designated owner and custodian, and location. Examples of applicable fields are given in Table 1, (organizations may choose the relevant fields).

8. Key performance indicators (KPIs) like maintenance completion, downtime, repair frequency, and Mean Time to Repair (MTTR) shall be tracked and reviewed at least once a year or as needed, to measure and improve the efficiency of asset maintenance.

9. New assets shall be acquired through an approved procurement process, including vendor evaluation, purchase authorization, and proper entry into the Asset Register.

10. Asset Register Sample format is provided in the Table 3.1 for reference:

Table 3.1: Asset Register

Asset Register				
Asset ID (A unique identifier for each asset, e.g., 001, 002)	**Asset Name** (The name of the asset, e.g., Laptop, Server)	**Asset Type** (Hardware, Software, etc.)	**Expected Life** (Anticipated duration before asset becomes obsolete, non-viable, or prone to failure)	**Make/Model** (Equipment details, e.g., company, model, etc.)
Owner (Responsible for defining requirements, ensuring proper use, and approving disposal)	**Custodian** (Responsible for physical care, day to day maintenance, and documentation)	**Location** (Where the asset is physically located, e.g., Office 101, Data Center)	**Department** (Department using or managing the asset, e.g., IT, HR)	**Condition** (Current physical condition, e.g., Excellent, Good, Fair)
Disposal Date (Planned or actual date when the asset is no longer in use)	**Warranty Status** (Expiry date of manufacturer's	**Asset Status** (Current operational status, e.g.,	**Confidentiality (0–5)** (How sensitive the information	**Integrity (0–5)** (How critical the accuracy of the

Muhammad Ismail Abdullah
Dr. Muhammad Ismail Abdullah
Secretary ICT
Director ICT
16 October 2026 03:22:11 PM

	warranty, if applicable)	Active, Inactive, Under Maintenance)	handled by the asset is)	data handled by the asset is)
Availability (0-5) (The importance of uptime/accessibility of the asset)	**Asset Value w.r.t CIA** (Security importance considering Confidentiality, Integrity, Availability)	**Security Controls** (List security measures implemented, e.g., Antivirus, Firewalls, IDS/IPS)	**Classification Level** (Sensitivity level based on data handled, business function supported, and potential impact)	**Notes** (Additional comments: handling requirements, known issues, or other information)

11. Decommissioning of information assets shall require documented authorization by the designated asset owner and compliance with the regulatory, and archival retention requirements of the organization.

12. All decommissioned assets shall undergo approved data sanitization or destruction procedures, termination of logical and physical access, and formal closure in organizational asset register.

13. To support audits, compliance, and accountability, all lifecycle records must be kept securely and for the set amount of time. This includes purchase records, usage logs, upgrade details, maintenance history, and disposal certificates.

3.3 Software and License Management

14. All licensed software assets shall be regularly updated. The administration of patches for licensed software shall be maintained with clearly defined roles and responsibilities.

15. The organization shall enforce a controlled and auditable process for software decommissioning, including stakeholder notification and data retention in compliance with regulatory and information security requirements.

PKCERT

3.4 System Categorization and Classification

16. Standardized classification levels based on the asset's sensitivity, business impact, and regulatory requirements shall be applied, and the security measures shall be implemented based on the asset's classification level.

17. Following classification scheme can be adopted (Table 3.2), where Most Critical, Highly Critical, Critical, non-Critical are based on severity.

Table 3.2: Classification Scheme

Level	Impact of compromise
Most Critical	**Catastrophic**, can result in extreme safety threats, extreme financial damage, or complete business shut down.
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.

18. This classification can also be understood while mapping it to confidentiality, integrity and availability (CIA) as given in Table 3.3

Table 3.3: Classification mapping with Impact on CIA

Impact on CIA	Non-critical	Critical	Highly Critical	Most Critical
Confidentiality Preserving authorized restrictions on information access and	The unauthorized disclosure of information could be expected to have	The unauthorized disclosure of information could be expected to	The unauthorized disclosure of information could be expected to	The unauthorized disclosure of information could be expected to

Muhammad Ismail Abdullah
Section Officer
13 October 2026 03:05:43 PM
PKCERT

disclosure, including means for protecting personal privacy and sensitive information.	**no specific or limited** adverse impact on operations, assets or individuals.	have **considerable** adverse impact on operations, assets or individuals.	have **serious** adverse impact on operations, assets or individuals.	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**	The disruption of access to or use of information or an information system could be expected to have a	The disruption of access to or use of information or an information system could	The disruption of access to or use of information or an information system could be expected to have a **severe**

Muhammad Hussain Abdullah
Director Officer
16 October 2026 03:02:43 PM
PKCERT

	no-specific impact on operations, assets or individuals.	**considerable/ noticeable** impact on operations, assets or individuals.	be expected to have a **serious** impact on operations, assets or individuals.	**or catastrophic** impact on operations, assets or individuals. (Unavailability may affect public safety, disruption in a 24/7 service etc.).

19. However, if the organization is not offering any services, then the classification may also be adopted for confidentiality as in Table 3.4.

20. The organization shall conduct periodic and event driven reviews of all systems to ensure classification levels remain aligned with data sensitivity, business impact, regulatory requirements, and security posture. Reviews shall be triggered by major system changes, security incidents, regulatory updates, or organizational restructuring.

21. The organization can formulate its own classification scheme in line with its objectives.

Table 3.4: Classification Scheme

Classification Level	Definition
Top Secret	Information of the highest sensitivity. Unauthorized disclosure could cause **severe harm**.
Confidential	Sensitive internal information Disclosure could cause **moderate to high impact**.
Internal Use Only	Non-public information intended for internal use. Risk is **limited if disclosed**.
Public	Approved for public access. Disclosure causes **no harm** to the organization.

Muhammad Ussain Afzal Ullah
Sr. Director (CERT)
14 October 2026 02:23:43 PM
KCERT

3.5 Risk Management

22. The organization shall systematically identify and maintain an inventory of all information assets, along with associated vulnerabilities, and potential threats to establish a comprehensive risk profile.

23. The organization shall conduct information security risk assessments using a structured and adaptable approach, allowing assessment at the level of asset, service, process, or scenario levels, and implementing defined likelihood and impact criteria across confidentiality, integrity, and availability (CIA).

24. Identified risks shall be analyzed, assigned quantitative or qualitative values, categorized (e.g., Low, Medium, High, Critical), and formally recorded in the risk register to enable prioritization for treatment in line with organizational objectives.

25. Each identified risk shall be assigned a designated risk owner responsible for ensuring appropriate risk evaluation, treatment, monitoring, and reporting throughout the risk lifecycle.

26. The organization shall establish and maintain a structured risk acceptance process, ensuring that residual risks are explicitly evaluated against defined risk appetite and tolerance levels, formally approved by authorized risk owners, and documented with justification. Approved risk acceptance and exceptions shall be linked to control selection, treatment prioritization, and periodic review.

27. Essential attributes for risk register shall be recorded, including applicable fields, like the fields given in Table 3.5 (organizations may choose the relevant fields):

Muhammad Usama Abdullah
14 October 2026 03:03:43 PM
PKCERT

Table 3.5: Attributes for Risk Register

Asset ID (Unique identifier linked from the Asset Register	Asset Details (Name, Model)	Vulnerability (Weaknesses in the asset e.g. pirated software, outdated AV)	Threat (Malicious actions that can harm an asset)	Likelihood (Chance of the risk occurring)	Impact (Severity of the consequence if it occurs)	Risk Rating (Combined level of risk based on likelihood and impact)	Last Review Date
Risk ID (Unique identifier for the risk)	Risk Description (What could go wrong)	Risk Category (Type of risk: operational, financial, etc.)	Risk Level (Level assigned as per a predetermined criteria)	Date Identified	Risk Owner (Person responsible for overseeing the risk)	Treatment Strategy (Approach: Mitigate, Accept, Transfer, Avoid)	Review Frequency
Treatment Actions (Steps/Controls planned to address the risk)	Action Owner (Person executing the treatment actions)	Target Completion Date	Residual Risk Rating (Remaining risk after treatment)	Controls Implemented (Specific controls to mitigate the risk)	Resources Needed	Status	Notes/ Comments

28. The organization shall define and implement formal risk treatment strategies including mitigation, acceptance, transference, or avoidance, with clearly defined responsibilities, deadlines, and controls for each risk to ensure residual risks are reduced to acceptable levels.
29. The organization shall establish processes to continuously monitor risks, effectiveness of applied controls, and key risk indicators (like number of cyber incidents reported, instances of third-party vendors, duration of operational downtime, financial or operational penalties due to non-compliance with regulations, etc.).
30. The organization shall define and formally approve risk appetite statements for relevant risk categories, reflecting the level and type of risk the organization is willing to accept in pursuit of its objectives.
31. The organization shall establish measurable risk tolerance thresholds for each risk category to define acceptable levels of deviation from the approved risk appetite and to trigger escalation and management action when exceeded.
32. Risk acceptance decisions exceeding defined tolerance levels shall be formally documented, approved by the appropriate authority, and reviewed periodically. Accountability for accepted risks shall rest with the designated risk owner.

PKCERT

4 ESSENTIAL SECURITY TRAINING CONTROLS

4.1 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.

4.2 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 senior management, 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.

PKCERT

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.

Muhammad Mehdi Sarwar Hadullah
Secretary of Cert
16 October 2026 03:23:43 PM
PKCERT

5 ESSENTIAL SYSTEM AND COMMUNICATION PROTECTION CONTROLS

5.1 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.

5.2 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, Time bound access, monitoring, auditing, and preferably multi-factor authentication.

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

MuhammadHusenAbdullah
Director(CERT)
14 October 2026 03:23:41 PM
PKCERT

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.

5.3 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.

5.4 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.

Muhammad Ibrahim Afzal Ullah
Sr. Director (Cert)
14 October 2026 03:02:43 PM
PKCERT

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.

5.5 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.

5.6 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

6 ESSENTIAL IDENTITY AND ACCESS MANAGEMENT CONTROLS

6.1 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.

6.2 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.

Muhammad Hussain Abdullah
Section Officer(S)
14 October 2026 03:25:41 PM
PKCERT

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

6.3 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 like limited in duration, and is fully auditable, with privileged activities logged and monitored.

Muhammad Usman Abdullah
Sr. Director (CERT)
16 October 2026 03:25:03 PM
PKCERT

7 ESSENTIAL DATA PROTECTION AND PRIVACY CONTROLS

7.1 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.

7.2 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.

Muhammad Mehtab Ullah
Sr. Director (Cert)
14 October 2026 03:22:41 PM
PKCERT

8. Organizations shall establish and maintain a documented data retention schedule. An illustrative retention schedule template is provided in Table 7.1, as an example, to support consistent classification, retention, and disposal of data in accordance with legal, regulatory, and business requirements.

Table 7.1: 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			

7.3 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 collected, processed, 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.

PKCERT

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.

7.4 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.

Muhammad Ubaid Usman Abdullah
Sr. Director (CERT)
16 October 2026 03:03:43 PM
PKCERT

8 ESSENTIAL INCIDENT RESPONSE CONTROLS

8.1 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.

8.2 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.

Muhammad Hussain Afzal Hullah
Secretary of CERT
16 October 2026 03:08:03 PM
PKCERT

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.

8.3 Business Continuity Plan (BCP) (Applicability 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.

PKCERT

8.4 Disaster Recovery Plan (Applicability 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.

Muhammad Usman Abdullah
Sr. Director (Cert)
16 October 2026 03:25:03 PM
PKCERT

9 ESSENTIAL PHYSICAL SECURITY CONTROLS

9.1 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.

9.2 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.

Muhammad Usman Abdullah
Sr. Director (CERT)
16 October 2026 03:25:03 PM
PKCERT

10 ESSENTIAL DATA CENTRE AND WEB HOSTING SERVICES CONTROLS

10.1 Introduction

1. 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.

2. 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.

10.2 Data Center

3. 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.

4. 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.

MuhammadHisnaAfzalullah
Sr. Dir. Officer(S)
14 October 2026 03:25:03 PM
PKCERT

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.

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

6. 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.

7. 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.

10.3 Email and Web Hosting Services

8. 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.

9. 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.

10.4 Web Application Security

10. 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)

11. 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.

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

Muhammad Ubaid Ullah Afzal Dilawar Director (CERT) 16 October 2026 03:02:43 PM
PKCERT

13. 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.

10.5 Environmental Controls (Data Centers and Hosting Facilities)

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

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

PKCERT

22. 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.

Muhammad Usman Abdullah
Sr. Director (Cert)
16 October 2026 03:25:03 PM
PKCERT

11 ESSENTIAL SECURE SOFTWARE DEVELOPMENT LIFE CYCLE CONTROLS

11.1 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.

11.2 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.

MuhammadHussainAbdullah
Director(Certified)
14 October 2026 03:23:41 PM
PKCERT

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 as per PSS is performed for critical software and applications as part of the secure development and acquisition lifecycle.

Muhammad Usman Abdullah
Section Officer
16 October 2026 03:25:43 PM
PKCERT

12 ESSENTIAL SUPPLY CHAIN MANAGEMENT CONTROLS

12.1 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.

12.2 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

Muhammad Usman Abdullah
Director Office
14 October 2026 03:02:41 PM
PKCERT

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, data and evaluate risks related to acquiring products or services from hostile jurisdictions.

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.

PKCERT

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.

Muhammad Usman Abdullah
Sr. Director (CERT)
16 October 2026 03:25:03 PM
PKCERT

13 ESSENTIAL AUDIT CONTROLS

13.1 Introduction

1. Pakistan Information Security Framework: **"Essential Audit Controls"**, outlines the baseline of information security internal and external/ third party 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/ third party information security audits, in alignment with regulatory requirements and organizational objectives. Aim is to strengthen governance through independent information security audits and continuous improvement.

13.2 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/ third party 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/ third party 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.

MuhammadAlisenAfzabullah
SecretariatSeriQ
14 October 2026 03:25:03 PM
PKCERT

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

14 ESSENTIAL CII PROTECTION CONTROLS

14.1 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.

14.2 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.

PKCERT

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.

PKCERT

14.3 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 14.1: 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 14.2: 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	The unauthorized disclosure of information could be expected to have **no specific or**	The unauthorized disclosure of information could be expected to have **considerable**	The unauthorized disclosure of information could be expected to have **serious** adverse impact	The unauthorized disclosure of information could be expected to have **severe or catastrophic** adverse impact on

Muhammad Ismail Ismail Hullah
SeDirectorate(CIT)
18 October 2026 03:28:43 PM
PKCERT

privacy and sensitive information.	**limited** adverse impact on operations, assets or individuals.	adverse impact on operations, assets or individuals.	on operations, assets or individuals.	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	The disruption of access to or use of	The disruption of access to or use of	The disruption of access to or use of information or	The disruption of access to or use of information or an information

Muhammad Mustafa Abdullah
Section Officer
14 October 2026 03:23:43 PM
PKCERT

to and use of information.	information or an information system could be expected to have a **tolerable or no-specific** impact on operations, assets or individuals.	information or an information system could be expected to have a **considerable/ noticeable** impact on operations, assets or individuals.	an information system could be expected to have a **serious** impact on operations, assets or individuals.	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.).***

14.4 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.

PKCERT

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/ third party 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/ third-party 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

ANNEX-A PISF CONTROLS

Control Domain	Area	Sub-Area	Control Title	Requirement Map ID
Essential Governance Controls				
Domain 1	Governance Controls	Organizational Structure	Accountability Matrix (RACI) for Information security Governance, Risk, and Compliance	PISFID-001
Domain 1	Governance Controls	Organizational Structure	Establishment of Independent information security Function Reporting to Top Management	PISFID-002
Domain 1	Governance Controls	Organizational Structure	Information security Function Lead Designation	PISFID-003
Domain 1	Governance Controls	Organizational Structure	Formulation of a information security Steering Committee	PISFID-004
Domain 1	Governance Controls	Organizational Structure	Defined information security Roles, Responsibilities approved by Steering Committee	PISFID-005
Domain 1	Governance Controls	Organizational Structure	Appointment of Competent and Dedicated information security Professionals, separated from IT function	PISFID-006
Domain 1	Governance Controls	Organizational Structure	Incident Management Governance, Reporting, and Business Continuity Alignment	PISFID-007
Domain 1	Governance Controls	Organizational Structure	Proactive Monitoring of Information Systems, Security Audit management	PISFID-008

PKCERT

Domain 1	Governance Controls	Policy & Procedure	Information security Policies and Procedures approval and dissemination	PISFID-009
Domain 1	Governance Controls	Policy & Procedure	Alignment of Information Security Policy with Organizational Objectives, Standards and Guidelines	PISFID-010
Domain 1	Governance Controls	Leadership and Commitment	Information security Strategy Formulation and Roadmap	PISFID-011
Domain 1	Governance Controls	Leadership and Commitment	Resource Allocation for Information Security	PISFID-012
Domain 1	Governance Controls	Leadership and Commitment	Top Management Leadership, Commitment, and Support for Information Security	PISFID-013
Domain 1	Governance Controls	Change Management	Secure, Structured, and Controlled Change Management Process	PISFID-014
Domain 1	Governance Controls	Change Management	Information Security Review and Risk Assessment of Proposed Changes	PISFID-015
Domain 1	Governance Controls	Change Management	Change Authorization and Emergency Change Governance	PISFID-016
Domain 1	Governance Controls	Compliance and Third-Party Management	Inventory of Applicable Legal, Regulatory, and Contractual Requirements	PISFID-017

PKCERT

Domain 1	Governance Controls	Compliance and Third-Party Management	Independent Internal Audit Function for Compliance Management and Reporting	PISFID-018
Domain 1	Governance Controls	Compliance and Third-Party Management	Third-Party Security Compliance Evaluation and Assurance	PISFID-019
Essential Asset & Risk Management				
Domain 2	Assets and Risk Management Controls	Asset Management	Identification, Classification, and Documentation of IT Assets	PISFID-020
Domain 2	Assets and Risk Management Controls	Asset Management	Ownership, Recordkeeping, and Lifecycle Management of IT Assets	PISFID-021
Domain 2	Assets and Risk Management Controls	Asset Management	Recording of Essential Asset Metadata in the Asset Register	PISFID-022
Domain 2	Assets and Risk Management Controls	Asset Management	Monitoring and Evaluation of Asset KPIs - downtime, MTTR etc.	PISFID-023
Domain 2	Assets and Risk Management Controls	Asset Management	Approved Asset Acquisition Process with Asset Register Documentation	PISFID-024
Domain 2	Assets and Risk Management Controls	Asset Management	Secure Decommissioning and Disposal of Assets	PISFID-025
Domain 2	Assets and Risk Management Controls	Asset Management	Asset Data Sanitization and Access Termination	PISFID-026

PKCERT

Domain 2	Assets and Risk Management Controls	Asset Management	Management and retention of Complete Asset Lifecycle Records	PISFID-027
Domain 2	Assets and Risk Management Controls	Software and License Management	Licensed Software Governance, Sustainment, and Patch Management	PISFID-028
Domain 2	Assets and Risk Management Controls	Software and License Management	Controlled and Auditable Software Decommissioning Process	PISFID-029
Domain 2	Assets and Risk Management Controls	System Categorization & Classification	Periodic and Event-Driven Review of System Classification and Data Sensitivity to Ensure Security Control Alignment with Asset Classification	PISFID-030
Domain 2	Assets and Risk Management Controls	Risk Management	Risk Profiling of Information Assets	PISFID-031
Domain 2	Assets and Risk Management Controls	Risk Management	Structured Information Security Risk Assessment and Risk Analysis	PISFID-032
Domain 2	Assets and Risk Management Controls	Risk Management	Defined Risk Ownership and Oversight	PISFID-033
Domain 2	Assets and Risk Management Controls	Risk Management	Risk Acceptance and Residual Risk Approval Process	PISFID-034
Domain 2	Assets and Risk Management Controls	Risk Management	Risk Treatment Planning and Execution	PISFID-035

PKCERT

Domain 2	Assets and Risk Management Controls	Risk Management	Continuous Risk and Control Effectiveness Monitoring	PISFID-036
Domain 2	Assets and Risk Management Controls	Risk Management	Establishment and Monitoring of Risk Appetite, Tolerance Thresholds and Escalation Triggers.	PISFID-037
Domain 2	Assets and Risk Management Controls	Risk Management	Documented Risk Acceptance Exceeding Thresholds	PISFID-038
Essential Security Training				
Domain 3	Essential Security Training Controls	Security Training	Structured information security Training and Awareness Program	PISFID-039
Domain 3	Essential Security Training Controls	Security Training	Mandatory Employee information security Awareness and Training (On boarding, Regular, Requirement Based)	PISFID-040
Domain 3	Essential Security Training Controls	Security Training	Role-Based Information Security and IT Training	PISFID-041
Domain 3	Essential Security Training Controls	Security Training	Specialized Role-Based Security Training for Privileged and High-Risk Roles	PISFID-042
Domain 3	Essential Security Training Controls	Security Training	Periodic Review and Update of Specialized Security Training Requirements	PISFID-043
Domain 3	Essential Security Training Controls	Security Training	Information security Awareness Program	PISFID-044

PKCERT

Domain 3	Essential Security Training Controls	Security Training	Documentation of information security Training Records and Performance Monitoring (Feedback, Audit etc.)	PISFID-045
Domain 3	Essential Security Training Controls	Security Training	Evaluation of Information Security Training Effectiveness	PISFID-046
Domain 3	Essential Security Training Controls	Security Training	Continuous Improvement of Security Training and Awareness	PISFID-047
Essential System and Communication Protection Controls				
Domain 4	Essential System & Communication Protection Controls	Network Security	Documented and approved network security requirements and security controls implementation	PISFID-048
Domain 4	Essential System & Communication Protection Controls	Network Security	Physical Protection of Network Infrastructure	PISFID-049
Domain 4	Essential System & Communication Protection Controls	Network Security	Implementation of Network Segmentation and Access Restrictions	PISFID-050
Domain 4	Essential System & Communication Protection Controls	Network Security	Perimeter Access Control and Threat Prevention (Firewall, IDS/IPS etc.)	PISFID-051

PKCERT

Domain 4	Essential System & Communication Protection Controls	Network Security	VPNs and MFA for Remote Access Security and Authentication Controls	PISFID-052
Domain 4	Essential System & Communication Protection Controls	Network Security	Critical internal resources Segregation from Wireless Network	PISFID-053
Domain 4	Essential System & Communication Protection Controls	Network Security	Controlled and Segmented Internet Access	PISFID-054
Domain 4	Essential System & Communication Protection Controls	Network Security	Network Activity Logging, Monitoring, and Audit Controls	PISFID-055
Domain 4	Essential System & Communication Protection Controls	Network Security	Network Security Baseline for Configuration Management	PISFID-056
Domain 4	Essential System & Communication Protection Controls	Protection of End Point Computing Devices	Endpoint Security Requirements Definition, Approval and Implementation	PISFID-057
Domain 4	Essential System & Communication Protection Controls	Protection of End Point Computing Devices	Endpoint Security and Malware Protection	PISFID-058

Muhammad Hussein Abdullah
Director (CCIP)
14 October 2026 03:02:43 PM
PKCERT

Domain 4	Essential System & Communication Protection Controls	Protection of End Point Computing Devices	External Storage Media Usage Controls and Protection	PISFID-059
Domain 4	Essential System & Communication Protection Controls	Protection of End Point Computing Devices	Endpoint Patch Management and Security Update	PISFID-060
Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Security Event Logging and Monitoring	PISFID-061
Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Continuous Aggregation and Monitoring Cyber Security Logs of all critical assets	PISFID-062
Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Centralized Security Logging and Event Monitoring	PISFID-063
Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Event Log Retention and Preservation Requirements	PISFID-064
Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Time Synchronization (NTP)	PISFID-065

PKCERT

Domain 4	Essential System & Communication Protection Controls	Event Logs & Monitoring	Log Integrity Preservation and Tamper Protection	PISFID-066
Domain 4	Essential System & Communication Protection Controls	Backup & Recovery Management	Backup and Recovery formal documentation and Implementation	PISFID-067
Domain 4	Essential System & Communication Protection Controls	Backup & Recovery Management	Backup and Recovery parameters RPO, RTO defined, implemented and tested	PISFID-068
Domain 4	Essential System & Communication Protection Controls	Backup & Recovery Management	Secure Backup Media and Storage Management	PISFID-069
Domain 4	Essential System & Communication Protection Controls	Backup & Recovery Management	Backup Restoration Testing and Integrity Verification	PISFID-070
Domain 4	Essential System & Communication Protection Controls	Backup & Recovery Management	Continuous Monitoring and Audit of Backup and Restore Activities	PISFID-071
Domain 4	Essential System & Communication Protection Controls	Vulnerability & Patch Management	Vulnerability management and Patch Management Program documented and implemented.	PISFID-072

PKCERT

Essential Identity and Access Management Controls				
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Documented and approved Identity Management policy and procedures	PISFID-073
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	User and Service Account Lifecycle Management	PISFID-074
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Risk Based Adaptive Authentication Management - Passwords, MFA etc.	PISFID-075
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Secure Credential Lifecycle Management	PISFID-076
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Role based access controls, reviewed and monitored	PISFID-077
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Access Authorization based on principle of least privilege.	PISFID-078
Domain 5	Essential Identity & Access Management Controls	Identity & Access Management	Centralized Management of Official Social Media Accounts	PISFID-079
Domain 5	Essential Identity & Access Management Controls	Privileged Access Management	Privileged Account Governance and Access Control	PISFID-080
Domain 5	Essential Identity & Access Management Controls	Privileged Access Management	Emergency and Third-Party Privileged Access Control	PISFID-081
Essential Data Protection and Privacy Controls				
Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Privacy Governance and Data Protection	PISFID-082

PKCERT

Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Management of personal data Collection and Processing with Consent	PISFID-083
Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Privacy Impact Assessment (PIA) for new systems, projects or processes.	PISFID-084
Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Documented Data Privacy Policy based on privacy principles	PISFID-085
Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Monitoring and Logging of Personal data Access and Activities	PISFID-086
Domain 6	Essential Data Protection & Privacy Controls	Data Privacy	Data Retention Schedule	PISFID-087
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Data Classification and protection	PISFID-088
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Documented procedures for Security of Personal and Organizational Data (At rest and in transit)	PISFID-089
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Role-Based Access of data	PISFID-090
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Encryption of data classified as Critical and Highly Critical	PISFID-091
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Data Integrity Management Across the Information Lifecycle	PISFID-092
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Data Retention and Secure Disposal	PISFID-093

PKCERT

Domain 6	Essential Data Protection & Privacy Controls	Data Security	Data Backup & Recovery Management	PISFID-094
Domain 6	Essential Data Protection & Privacy Controls	Data Security	Data Access and Security Event Monitoring and Logging	PISFID-095
Domain 6	Essential Data Protection & Privacy Controls	Data Breach	Continuous Monitoring of Systems and Networks for Data Breach Detection	PISFID-096
Domain 6	Essential Data Protection & Privacy Controls	Data Breach	Data breach detection, containment and Impact Control	PISFID-097
Domain 6	Essential Data Protection & Privacy Controls	Data Breach	Notification of Data Breaches	PISFID-098
Domain 6	Essential Data Protection & Privacy Controls	Data Breach	Policy and procedure for notifying Affected Individuals for Personal Data Breaches	PISFID-099
Domain 6	Essential Data Protection & Privacy Controls	Data Breach	Policy and procedure for Controlled and Coordinated Public Disclosure of Data Breaches	PISFID-100
Essential Incident Response Controls				
Domain 7	Essential Incident Response Controls	Incident Management	Documented Incident Response Management Policy and Procedures	PISFID-101
Domain 7	Essential Incident Response Controls	Incident Management	Classification of Security Incidents by Severity and Impact	PISFID-102
Domain 7	Essential Incident Response Controls	Incident Management	Information Security Incident Management ownership and accountability	PISFID-103

PKCERT

Domain 7	Essential Incident Response Controls	Incident Management	Network Monitoring, SOC SIEM Solutions based on the requirement of the organization	PISFID-104
Domain 7	Essential Incident Response Controls	Incident Management	Incident Response Readiness and Testing	PISFID-105
Domain 7	Essential Incident Response Controls	Incident Management	Critical Infrastructure Incident Reporting to Sectoral Regulators and nCERT	PISFID-106
Domain 7	Essential Incident Response Controls	Incident Management	Non-Critical Infrastructure Incident Reporting to Sectoral Regulators	PISFID-107
Domain 7	Essential Incident Response Controls	Incident Management	Incident Lessons Learned and Corrective Action documented and implemented	PISFID-108
Domain 7	Essential Incident Response Controls	Business Continuity Plan	Business Continuity Program Governance and Coordination	PISFID-109
Domain 7	Essential Incident Response Controls	Business Continuity Plan	Business Continuity Strategy and Business Impact Analysis (BIA)	PISFID-110
Domain 7	Essential Incident Response Controls	Business Continuity Plan	Documented Business Continuity Plan Activation and Post-Incident Recovery Procedures	PISFID-111
Domain 7	Essential Incident Response Controls	Business Continuity Plan	Annual Business Continuity and Recovery Testing	PISFID-112
Domain 7	Essential Incident Response Controls	Disaster Recovery Plan	Disaster Recovery Plan Activation based on RTO and RPO	PISFID-113
Domain 7	Essential Incident Response Controls	Disaster Recovery Plan	Disaster Recovery Communication and Escalation Procedures	PISFID-114

PKCERT

Essential Physical Security Controls				
Domain 8	Essential Physical Security Controls	Physical Security Control	Documented and Implemented Physical Security for Information and Technology Assets	PISFID-115
Domain 8	Essential Physical Security Controls	Physical Security Control	Physical Access Control and Authorization to Sensitive Facilities	PISFID-116
Domain 8	Essential Physical Security Controls	Physical Security Control	Documented Controlled Physical Access to Organizational Facilities	PISFID-117
Domain 8	Essential Physical Security Controls	Physical Security Control	Physical Surveillance Systems for Security Monitoring	PISFID-118
Domain 8	Essential Physical Security Controls	Physical Security Control	Perimeter Security Controls	PISFID-119
Domain 8	Essential Physical Security Controls	Physical Security Control	Physical Access Records Monitoring and Storage	PISFID-120
Domain 8	Essential Physical Security Controls	Physical Security Control	Secure and documented Disposal and Reuse of Classified Information Assets	PISFID-121
Domain 8	Essential Physical Security Controls	Physical Security Control	Secure Removal of Storage Media Prior to External Maintenance	PISFID-122
Domain 8	Essential Physical Security Controls	Physical Security Control	Fire Safety and Response Controls	PISFID-123
Essential Supply Chain Controls				
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supply Chain Security Management policies and procedures	PISFID-124

PKCERT

Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supply Chain Risk Identification and Classification	PISFID-125
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Risk-Based Supply Chain Mitigation Strategies	PISFID-126
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Continuous Monitoring and Review of Supply Chain Risks	PISFID-127
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Third-Party Service Provider Compliance Management	PISFID-128
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Identification, Classification, and Documentation	PISFID-129
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Documented Supplier Due Diligence and Pre-Engagement Security Assessment	PISFID-130
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Security Clauses in Supplier Contract (SLAs) and Confidentiality Agreements (NDAs)	PISFID-131
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Accountability for Third-Party Accepted Risks	PISFID-132
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Transparency and Provenance Verification	PISFID-133
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Data Protection and Privacy Compliance	PISFID-134
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Compliance Monitoring and Oversight	PISFID-135

PKCERT

Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier security incident response and reporting mechanisms	PISFID-136
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Business Continuity and Disaster Recovery Management	PISFID-137
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supplier Accountability for Subcontractor	PISFID-138
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Secure Supplier Offboarding and Contract Termination Management	PISFID-139
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supply Chain Risk Reassessment upon Significant Supplier Changes	PISFID-140
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supply Chain Concentration Risk Management	PISFID-141
Domain 9	Essential Supply Chain Controls	Supply Chain Controls	Supply Chain Risk Management Training for Procurement Personnel	PISFID-142
Essential Audit Controls				
Domain 10	Essential Audit Controls	Information Security Audit	Internal and External Audit Function	PISFID-143
Domain 10	Essential Audit Controls	Information Security Audit	Control Self-Assessment (CSA) Implementation	PISFID-144
Domain 10	Essential Audit Controls	Information Security Audit	Independent and Certified Information Security Auditors engagement	PISFID-145

PKCERT

Domain 10	Essential Audit Controls	Information Security Audit	Confidentiality and Data Protection in Audit Engagements	PISFID-146
Domain 10	Essential Audit Controls	Information Security Audit	Risk-Based information security Audit Planning and Execution	PISFID-147
Domain 10	Essential Audit Controls	Information Security Audit	Documented Audit Planning and Executive Approval	PISFID-148
Domain 10	Essential Audit Controls	Information Security Audit	Provision of accurate and up to-date Audit related Documents	PISFID-149
Domain 10	Essential Audit Controls	Information Security Audit	Standardized Assessment with verifiable and sufficient audit evidences	PISFID-150
Domain 10	Essential Audit Controls	Information Security Audit	Audit Results Reporting and Stakeholder Communication	PISFID-151
Domain 10	Essential Audit Controls	Information Security Audit	Audit Closure and Corrective Action Management	PISFID-152
Domain 10	Essential Audit Controls	Information Security Audit	Audit Framework Review and Continuous Enhancement	PISFID-153
Essential Data Center and Web Hosting Services Controls				
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center Physical Security, Access Control and Surveillance Measures	PISFID-154

PKCERT

Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Network and Perimeter Security as per the requirement and risk assessment	PISFID-155
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Server Hardening and Secure Configuration Management	PISFID-156
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center Patch and Vulnerability Management	PISFID-157
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Business Continuity and Disaster Recovery Planning and Testing	PISFID-158
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center and Web Hosting Security Monitoring, SIEM, SOC	PISFID-159
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center Structured Cabling and Infrastructure Management	PISFID-160
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center critical Log Retention and Audit Trail Management	PISFID-161

Muhammad Usman Abdullah
Director (Q)
14 October 2026 03:02:43 PM
PKCERT

Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Secure Backup and Recovery Controls	PISFID-162
Domain 11	Essential Data Center & Web Hosting Services Controls	Data Center	Data Center Audit (Internal and External) and Compliance Assurance	PISFID-163
Domain 11	Essential Data Center & Web Hosting Services Controls	Email & Web Hosting Services	Advanced Email Threat Protection	PISFID-164
Domain 11	Essential Data Center & Web Hosting Services Controls	Email & Web Hosting Services	MFA for Administrative, Remote, and Webmail Access	PISFID-165
Domain 11	Essential Data Center & Web Hosting Services Controls	Email & Web Hosting Services	Email Archiving, Backup, and Restoration Controls	PISFID-166
Domain 11	Essential Data Center & Web Hosting Services Controls	Email & Web Hosting Services	Advanced Threat Detection and Response	PISFID-167
Domain 11	Essential Data Center & Web Hosting Services Controls	Email & Web Hosting Services	Email Domain Authentication (SPF, DKIM, DMARC or equivalent)	PISFID-168

PKCERT

Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Web Application Security documentation and implementation	PISFID-169
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Web Application Access Control	PISFID-170
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Secure Application Architecture and Layered Defense	PISFID-171
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Secure Communication Protocols for Data in Transit	PISFID-172
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Secure Usage and User Awareness Controls	PISFID-173
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	VA/PT and follow up actions of Web Applications and Systems	PISFID-174
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Secure Maintenance and Patching of Web Application	PISFID-175

Muhammad Hussain Abdullah
Director (Cyber)
16 October 2026 03:02:43 PM
PKCERT

Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Authentication for Externally Accessible Web Applications	PISFID-176
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Secure Web Application Development and Pre-Deployment Security Testing	PISFID-177
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Data Residency and Local Hosting Requirement	PISFID-178
Domain 11	Essential Data Center & Web Hosting Services Controls	Web Application Security	Developer and Cloud Service Provider SLAs for Responsibility and Accoutability	PISFID-179
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Environmental Controls- Monitoring and alerting for Data Center Protection	PISFID-180
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Data Center Power Supply Resilience	PISFID-181
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	HVAC Controls for Data Center Environmental Management	PISFID-182

PKCERT

Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Data Center Fire Safety and Suppression Systems	PISFID-183
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Physical and Environmental Hazard Controls for Data Centers	PISFID-184
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Environmental Management Procedures and Roles for Data Centers	PISFID-185
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Testing and Audit of Environmental Control Systems	PISFID-186
Domain 11	Essential Data Center & Web Hosting Services Controls	Environmental Controls	Environmental Incident Logging and Management	PISFID-187
Essential SSDLC Controls				
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Documented Secure Software Development Life Cycle (SSDLC) Implementation	PISFID-188
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Security Integration in Design Phase of Software Development	PISFID-189

Muhammad Usman Abdullah
Section Officer(S)
16 October 2026 03:22:43 PM
PKCERT

Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Secure Code Review and Approval	PISFID-190
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Role-Based training for Secure Coding, Development and evaluation	PISFID-191
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Segregation of Development, Testing and Production Environment	PISFID-192
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Secure Source Code and Configuration Repository Management	PISFID-193
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Pre-Integration Security Assessment of External Software Components	PISFID-194
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Secure Tools for Continuous Code Scanning and Vulnerability Management	PISFID-195
Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Security and Functionality Testing Before final Deployment	PISFID-196

PKCERT

Domain 12	Essential Secure Software Development Lifecycle Controls	SSDLC Controls	Independent Security Testing for Critical Software	PISFID-197
Essential Critical Information Infrastructure Protection (CIIP) Controls				
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Information Security Governance and Resource Management	PISFID-198
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	CII Ownership Responsibility and Accountability for Security Governance	PISFID-199
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Procedure for Notifying Regulator Regarding Change	PISFID-200
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Information security Function Lead Designation	PISFID-201
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Formulation of a information security Steering Committee	PISFID-202

Muhammad Usman Abdullah
Director CerQ
14 October 2026 03:02:43 PM
PKCERT

Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Defined information security Roles, Responsibilities approved by Steering Committee	PISFID-203
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Appointment of Competent and Dedicated information security Professionals	PISFID-204
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Independent IT and Cybersecurity Function Establishment	PISFID-205
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Cybersecurity Steering Committee Reporting to Top Management	PISFID-206
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Assignment and Communication of CII Cybersecurity Roles and Responsibilities	PISFID-207
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	Approval and Authorization of Cybersecurity Roles and Responsibilities	PISFID-208
Domain 13	Essential CIIP Controls	Governance & Resource Allocation	CII Specific Cybersecurity Framework and Policy Development	PISFID-209

Muhammad Hussain Abdullah
Sub Director (IT)
14 October 2026 03:02:43 PM
PKCERT

Domain 13	Essential CIIP Controls	Governance & Resource Allocation	CII Risk Assessment and Risk-Driven Security Control Management	PISFID-210
Domain 13	Essential CIIP Controls	Critical Asset Classification Framework	Classification of Assets (Most Critical, Highly Critical, Critical, or Non-Critical) based on CIA	PISFID-211
Domain 13	Essential CIIP Controls	Critical Asset Classification Framework	Documented Security Control Alignment with Asset Classification	PISFID-212
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Risk-Based Implementation and Prioritization of Cybersecurity Controls for CII	PISFID-213
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Implementation and Testing of Information Security Controls for CII	PISFID-214
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Personal Data Protection and Retention Compliance	PISFID-215
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Security by Design for CII Systems and Facilities	PISFID-216

PKCERT

Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Physical and Environmental Security Policy and Planning for CII	PISFID-217
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Management of information security resilience and continuity for Critical Information Infrastructure.	PISFID-218
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Establishment and Approval of Business Continuity and Disaster Recovery Plans for CII	PISFID-219
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Resilience and Stress Testing of Critical Infrastructure	PISFID-220
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Recovery and Response Metrics for Critical Systems	PISFID-221
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Approval and Risk-Based Validation of BCP and DRP	PISFID-222
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Backup Restoration Testing and Single Point of Failure Mitigation	PISFID-223

PKCERT

Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	CII Supply Chain Risk Assessment and Procurement Security Validation	PISFID-224
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	CII Internal and External Audit Governance and Compliance Oversight	PISFID-225
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Documented CII Audit Confidentiality SOPs	PISFID-226
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Structured Incident Management and Response Framework for CII	PISFID-227
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	CII Coordination with sectoral CERT	PISFID-228
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Incident Response Planning and Management for CII	PISFID-229
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Threat Intelligence and Incident Escalation Mechanism to Sectoral CERTs	PISFID-230

Muhammad Hussain Abdullah
Sr. Director (CERT)
1st October 2026 03:02:43 PM
PKCERT

Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Procedure for Reporting of CII information security Incidents to Sectoral CERT (72 hours)	PISFID-231
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	SOPs for CII Coordination with organizational, sectoral, and national CERTs.	PISFID-232
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	Information security Awareness and Training for CII Employees	PISFID-233
Domain 13	Essential CIIP Controls	CIA-Aligned Control Implementation	National and International Cyber Threat Intelligence Linkages for CIIs	PISFID-234

Muhammad Usman Abdullah
Section Officer
16 October 2026 03:02:43 PM
PKCERT

PKCERT

Safeguarding Pakistan's Cyberspace

Muhammad Hussain Abdullah
Director (IT)
Director Office
14 October 2026 03:25:43 PM

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