PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

NTISB

A. INTRODUCTION

1. **"Pakistan Information Security Framework (PISF) 2025"**, outlines the baseline of information security controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs. The aim of the framework is to provide essential cybersecurity controls that all federal departments shall implement to ensure compliance with the cybersecurity implementation requirements issued from time to time by National Telecommunication and Information Technology Board (NTISB), National Computer Emergency Response Team (nCERT) and established through National Cyber Security Policy 2021 and CERT Rules 2023.

2. PISF 2025 is comprised of following 13 policy documents:

(1) Essential Governance Controls

(2) Essential Asset & Risk Management Controls

(3) Essential Security Training Controls

(4) Essential System and Communication Protection Controls

(5) Essential Identity and Access Management Controls

(6) Essential Data Protection and Privacy Controls

(7) Essential Incident Response Controls

(8) Essential Physical Security Controls

(9) Essential Data Centre and Web Hosting Services Controls

(10) Essential Secure Software Development Life Cycle Controls

(11) Essential Supply Chain Management Controls

(12) Essential Audit Controls

(13) Essential CII Protection Controls

B. APPLICABILITY

3. This policy framework shall be applicable to all Federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

4. Throughout the document "organization" is used to refer any of the above.

5. Scale and size of the implementation will vary and will be according to the size of the organization.

C. IMPLEMENTATION ECHO SYSTEM

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

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

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

9. **Oversight and Compliance**. Oversight audits shall be performed by nCERT/ NTISB for compliance assessment.

D. IMPLEMENTATION ROAD MAP

10. The implementation roadmap outlines a phased approach to establishing and maintaining a robust security posture across the organization:

11. **Phase 1 Essential Governance Controls:** Define policies, responsibilities and oversight mechanisms to establish the foundation for essential security.

12. **Phase 2 Essential Asset & Risk Management Controls:** Identify, evaluate, and protect critical assets through effective risk management practices.

13. **Phase 3 Essential Core Controls:** System and communication protection, identity and access management, data protection and privacy, incident response, physical security, and supply chain management constitute the foundational security controls that every organization shall implement.

14. **Data Center and Web Hosting Services:** Applicable to organizations that operate their own data centers or utilize/provide web hosting services.

15. **Secure Software Development Life Cycle (SSDLC):** Applicable to organizations engaged in software design, development, or maintenance activities.

16. **Critical Information Infrastructure (CII) Protection:** Applicable to organizations or sectors designated as critical information infrastructure.

17. **Phase 4 Audit Controls:** Validate compliance, assess effectiveness, and drive continual improvement through structured audit processes.

18. **Security Training:** Training programs are embedded into each of the above mentioned phase to ensure employees have the knowledge and capabilities to effectively implement and sustain essential security controls.

Pakistan Information Security Framework (PISF) 2025
Implementation Roadmap

Phase 1

Essential Governance Controls

Phase 2

Essential Asset & Risk Management Controls

Phase 3

Essential System and Communication Protection Controls

Essential Identity and Access Management Controls

Essential Data Protection and Privacy Controls

Essential Incident Response Controls

Essential Physical Security Controls

Essential Data Centre and Web Hosting Services Controls *(Where Applicable)*

Essential Secure Software Development Life Cycle Controls *(Where Applicable)*

Essential Supply Chain Management Control

Essential CII Protection Controls *(Where Applicable)*

Phase 4

Essential Audit Controls

Essential Security Training Controls

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential System and Communication Protection Controls

NTISB

INTRODUCTION

Pakistan Information security Framework 2025: **"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. This policy applies to all organizational systems, networks, communication channels, and supporting technologies used to 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.

ESSENTIAL SYSTEM AND COMMUNICATION PROTECTION CONTROLS

A. NETWORKS SECURITY

1. Cybersecurity requirements for network security management shall be defined, documented, approved and implemented.

2. The organization shall establish and maintain a secure network architecture that ensures appropriate segregation, protection, and resilience in line with defense-in-depth principles and the organization's risk management strategy.

3. The cybersecurity requirements for network security management shall include at least the following:-

a) The organization shall ensure the physical protection of all network infrastructure and information assets to safeguard against unauthorized access, damage, or disruption.

b) The organization shall ensure appropriate segregation of networks to reduce security risks and prevent unauthorized access across different environments and functions

c) Appropriate perimeter security controls shall be implemented to block unauthorized access and detect/prevent threats (like Firewall, IDS/IPS as per the need decided by the steering committee of cyber security)

d) Remote connectivity on strict need basis shall be secured with appropriate measures, including VPNs, monitoring, auditing, and preferably multi-factor authentication, to protect against unauthorized access.

e) The organization shall ensure that wireless networks are securely managed and isolated from critical internal resources to prevent unauthorized access.

f) Internet access shall be granted only through systems that are segmented and protected by robust security controls to prevent unauthorized access and threats

g) The organization shall ensure that network activity is logged and monitored to support incident investigation, security auditing, and compliance requirements

h) A network security baseline and configuration shall be developed, with change management processes implemented to prevent unauthorized or malicious changes.

i) Regular reviews shall be conducted to detect and remediate deviations from the baseline, whether caused by unintentional errors or malicious activities

B. PROTECTION OF END POINT COMPUTING DEVICES

4. Cybersecurity requirements for protecting end point computing devices (Servers, workstations, Mobiles and Tablets etc.) shall be defined, documented, approved and implemented.

5. The cybersecurity requirements for protecting end point computing devices shall include at least the following:

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

b) Organizations shall restrict the use of external storage media and shall ensure that any permitted use is handled securely according to approved procedures.

c) Organizations shall maintain up-to-date end point computing devices through regular patch management and updates.

6. All BYOD/mobile devices accessing enterprise systems will be recorded manually or in an approved Mobile Device Management (MDM) platform including device registration, assignment of user or owner roles, verification of device health and OS compliance

7. Only authorized data will be accessed, stored, or processed on BYOD/mobile devices, according to the organization's Data Classification Policy. Any secret or confidential data will not be stored/ process on BOYD/mobile devices.

8. Log retention and compliance reporting for all enrolled BYOD/ Mobile Devices will be ensured.

C. EVENT LOGS AND MONITORING

9. Cybersecurity requirements for event logs and monitoring shall be defined, documented, approved and implemented.

10. Event log and monitoring requirements shall include following:-

a) Organizations shall ensure comprehensive event logging of, at a minimum, all critical assets, remote access connections and privileged user accounts.

b) Centralized log management and monitoring shall be implemented using technologies to aggregate, correlate, and continuously analyze cybersecurity events.

c) The organization shall retain 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) All systems shall synchronize clocks using NTP (Network Time Protocol) with a reliable and precise time source.

e) Active and archive logs shall be protected from unauthorized tampering, destruction, or alteration, whether intentional or unintentional, to ensure their integrity and accuracy.

f) The organization shall maintain a log management policy that ensures compliance, preserves required logs, and optimizes storage and system performance.

D. BACKUP AND RECOVERY MANAGEMENT

11. Cybersecurity requirements for backup and recovery management shall be defined, documented, approved and implemented.

12. Backup and recovery management shall ensure comprehensive coverage of critical technology and information assets, enable quick data and system recovery after cybersecurity incidents, and undergo periodic testing to verify recovery effectiveness.

E. VULNERABILITY AND PATCH MANAGEMENT

13. Cybersecurity requirements for vulnerabilities and patch management shall be defined, documented, approved and implemented.

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

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

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Supply Chain Controls

NTISB

INTRODUCTION

Pakistan Information security Framework 2025: **"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.

This policy 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.

ESSENTIAL SUPPLY CHAIN CONTROLS

A. SUPPLY CHAIN LIFE CYCLE MANAGEMENT

1. Organizations procuring services like cloud, Data Center, Web hosting, Secure software development etc. must ensure service providers comply with relevant policy frameworks in the PISF 2025 and/or applicable laws/ regulations (e.g cloud policy)
2. The organizations shall define and implement policies, procedures, and processes for managing supply chain risks for products, systems, and services provided by third parties.

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

4. The organization shall conduct due diligence on all suppliers prior to engagement to ensure compliance with security, legal, and regulatory requirements.

5. All supplier agreements must include contractual provisions addressing information security, data protection and confidentiality and compliance obligations.

6. The organization shall ensure transparency and verification of supplier provenance, including the origin and integrity of products, services, and data.

7. Suppliers must handle, process, and share organizational data strictly in accordance with approved security and privacy requirements (Ref: Data protection and privacy policy).

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

9. The organization shall require suppliers to demonstrate compliance with applicable legal, regulatory, and security standards through certifications, audits, or assessments, and shall enforce penalties for non-compliance.

10. Suppliers shall promptly detect, report, and coordinate with the organization on security incidents affecting data or services, following defined procedures, timelines, and joint response mechanisms.

11. Suppliers must maintain appropriate business continuity and disaster recovery capabilities to ensure resilience of critical services.

12. Suppliers shall remain accountable for the actions of their subcontractors and fourth parties, ensuring that equivalent security and compliance obligations are enforced.

13. Suppliers shall securely off board by returning or destroying data, revoking access, undergoing exit audits, and ensuring service continuity and data integrity during contract completion/ Termination.

B. SUPPLY CHAIN RISK MANAGEMENT

14. The organization shall identify and classify supply chain risks across defined categories using standardized methodologies, tools, and threat intelligence, with special emphasis on cybersecurity, third-party access, and critical supplier dependencies.

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

16. All identified supply chain risks shall be continuously monitored, tracked, and reviewed to ensure timely response and remediation.

17. The organization shall continuously monitor and track supply chain risks.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

ESSENTIAL SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC) CONTROLS

NTISB

INTRODUCTION

Pakistan Information security Framework 2025: **"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.

This policy 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 regulations and standards.

ESSENTIAL SSDLC CONTROLS

1. 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.

2. The requirements for SSDLC shall include at the least the following: -

   a) The organization shall embed security from the earliest stages of software development and ensure alignment with well-known standards, thereby minimizing vulnerabilities and preventing misconfigurations throughout the SDLC

   b) Security shall be integrated throughout the SDLC, from defining requirements through risk and compliance inputs to secure design, coding, testing, and deployment. All code shall undergo security validation before release, with post-implementation reviews ensuring continued compliance and resilience.

   c) The organization shall ensure that developers are appropriately trained in secure coding practices.

d) The organization shall maintain separate development, testing, and production environments.

e) The organization shall maintain secure repositories for source code and configuration items to ensure integrity, controlled access, and traceability throughout the SDLC.

f) All commercial, open-source, and third-party components (software libraries, modules, middleware, etc.) shall undergo security review and approval before acquisition and integration.

g) The organization shall adopt approved tools for code scanning, security testing, dependency management, and version control, integrated into the CI/CD pipeline to enable continuous security and early vulnerability detection.

h) All software and applications developed by the organization shall be comprehensively tested through expert code reviews and manual/automated assessments to ensure security, performance, and functionality prior to deployment.

i) Organizations without in-house testing capabilities shall engage Pakistan Security Standard (PSS) accredited laboratories to perform code testing and ensure compliance with established security standards.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Security Training Controls

NTISB

INTRODUCTION

Pakistan Information Framework 2025: **"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.

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

ESSENTIAL SECURITY TRAINING CONTROLS

1. The organization shall establish and maintain a structured cybersecurity training plan that defines priorities, topics, schedules, resources, delivery methods, and target audiences to ensure comprehensive coverage and program effectiveness aligned with recommendations from NTISB and nCERT and endorsed by top management of an organization.

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

3. Employees in IT and cyber security shall be trained and certified in role-specific IT & service management and cyber security to ensure competency.

4. 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.

5. Specialized training requirements shall be identified through risk assessments, audits, incidents, and regulatory obligations, and shall be refreshed periodically to maintain competency and address evolving technologies and threat landscapes.

6. Cybersecurity training shall address key areas such as password management, phishing, social engineering, secure remote work, mobile device security, data privacy, and incident reporting, delivered through multiple formats (e-learning, instructor-led sessions, webinars, tabletop exercises), with content reviewed and updated regularly based on evolving threats, regulatory updates, and lessons learned.

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

8. The organization shall evaluate the effectiveness of its cybersecurity training program through simulations, assessments, and performance monitoring, ensuring that outcomes directly inform corrective and preventive actions.

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

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Physical Security Controls

NTISB

INTRODUCTION

Pakistan Information security Framework 2025: **"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.

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

ESSENTIAL PHYSICAL SECURITY CONTROLS

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

2. The cybersecurity 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)

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

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

d) All storage media shall be removed from devices before sending them for repair outside the organization.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Incident Response Controls

INTRODUCTION

Pakistan Information security Framework 2025: **"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.

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

ESSENTIAL INCIDENT RESPONSE CONTROLS

A. INCIDENT MANAGEMENT

1. The organization shall establish cybersecurity incident management requirements, including incident response plans, escalation procedures, and classification of cybersecurity incidents based on severity and impact.

2. The organization shall formulate cyber security incident management policy and procedure for detection, response, mitigation, reporting, recovery, remediation of cyber security incidents.

3. The organizations other than service providers shall perform the need analysis and feasibility of establishment of security operations center (SOC) or acquiring SIEM and other relevant solutions.

4. Incidents shall be classified using a standardized severity model based on data sensitivity, system criticality, business impact, and managed through a recognized response framework to ensure clear ownership, accountability, and consistent processes.

5. The organization shall maintain readiness through clear policies, adequate resources, and skilled teams. All incidents shall be verified, analyzed,

and investigated using documented procedures, with defined processes for internal reporting and secure, timely communication with stakeholders.

6. Procedures shall be established for the systematic containment, eradication, and recovery from incidents, including evidence collection with a maintained chain of custody, root cause analysis, and restoration.

B. INCIDENT RESPONSE

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

8. The organization shall report cybersecurity 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.

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

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

10. The organization shall define and implement a comprehensive continuity strategy, including tiered recovery, alternate sites, remote work, and supply chain resilience, based on an annual Business Impact Analysis (BIA) that classifies functions and dependencies.

11. The BCP shall be activated for any incident disrupting critical functions, post-activation actions must follow documented procedures for damage assessment, communications, recovery, and restoration, with all activities logged.

12. The organization shall conduct annual simulations and quarterly exercises to test recovery capabilities, ensure compliance, and build resilience, with all tests evaluated against defined success criteria.

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

13. The Disaster Recovery Plan (DRP) shall be activated by the organization upon defined triggers such as primary site failure, critical application outages exceeding the Recovery Time Objective (RTO), data corruption, or severe security incidents. Recovery shall follow system-specific procedures based on priorities defined in the Business Impact Analysis (BIA), including validated backup restoration, evidence preservation for cyber incidents, and coordination with the organization's Incident Response and Backup policies
14. 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.
15. A comprehensive backup strategy with secure, offsite storage and defined retention periods shall be maintained. Quarterly restore tests of all critical systems shall be performed, and a lessons-learned review shall be conducted after each DR event or test to update plans and procedures.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Identity and Access Management Controls

NTISB

INTRODUCTION

Pakistan Information Security Framework 2025: **"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.

This document governs the management of all user, service, system, 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.

ESSENTIAL IAM CONTROLS

A. IDENTITY AND ACCESS MANAGEMENT

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

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

3. The organization shall enforce a centralized 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.

4. The organization shall enforce secure lifecycle management of all credentials, including password standards, encrypted storage, regular rotation, and immediate revocation upon compromise or termination.

5. The organization shall enforce the principle of least privilege through defined access control models, ensuring all access to systems and data is authorized based on business need and is formally approved, regularly reviewed, and promptly revoked upon role change or termination.

B. PRIVILEGED ACCESS MANAGEMENT

6. 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.

7. Emergency break-glass and third-party privileged access shall require enhanced approval, be time-bound and fully auditable, with all privileged activities recorded and continuously monitored through approved PAM tools to detect and prevent misuse.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Governance Controls

NTISB

INTRODUCTION

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

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

ESSENTIAL GOVERNANCE CONTROLS

A. POLICIES AND PROCEDURES

1. The cybersecurity function shall define, document, and implement cybersecurity policies and procedures[1], which must be approved and disseminated to relevant parties.

2. The cybersecurity policies and procedures must be aligned with the technical security standards, industry-recognized best practices and guidelines issued by nCERT from time to time.

B. LEADERSHIP AND COMMITMENT

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

(a) A cybersecurity strategy shall be defined, documented and approved by Competent Authority. It shall be supported by the head of the

[1] The national CERT (nCERT) has provided customizable policy templates for organizations to scope and tailor according to their specific context and requirement.

organization and his/her delegate. The strategy goals shall be in-line with related laws and regulations.

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

(c) Top management shall ensure establishing an organizational structure that supports information security governance and operations, ensuring availability of skilled human resources, planning and allocation of sufficient financial resources to support effective information security operations.

(d) Top management shall lead information security efforts by communicating importance, ensuring mandatory security trainings, ensuring effectiveness, directing personnel, driving improvement, and supporting cybersecurity teams to achieve a robust security posture aligned with organizational risk level or sensitivity.

C. ORGANIZATIONAL STRUCTURE

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

5. A steering committee for cyber security matters shall be formulated and notified headed by the top management of the organization, responsible for making all cyber security related decisions.

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

7. Cyber security function lead (CISO, CIO, CRO, Min BS-20 or equivalent) shall be designated and made part of the steering committee of the organization responsible for all technology related decision making.

8. Steering committee shall define, document, approve, and assign cybersecurity roles, and responsibilities, ensuring no conflict of interest arises from these assignments. RACI matrix (Responsible, Accountable, Consulted, and Informed) for all data, systems and processes shall be maintained.

9. The position of cybersecurity function lead, related supervisory and critical positions within the function, must be filled with full-time and requisite experienced cybersecurity 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 cybersecurity steering committee shall provide regular reports to top management to ensure informed decision-making and alignment with organizational risk management strategies.

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

13. The organization shall establish governance mechanisms to ensure internal and external audits are conducted, review and address audit outcomes, implement remediation measures, and maintain complete audit trails and documentation.

D. CHANGE MANAGEMENT

14. The organization shall govern changes through defined types, request processes, and structured implementation, testing, and review to ensure secure and controlled operations.

15. The organization shall maintain configuration baselines and integrity checks, and govern patch evaluation, approval, deployment, rollback, and release processes to ensure systems remain secure, consistent, and reliable.

E. COMPLIANCE AND THIRD-PARTY MANAGEMENT

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

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

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

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Data Protection and Privacy Controls

NTISB

INTRODUCTION

"Pakistan Information Security Framework 2025: **"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.

This policy 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. The policy 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.

ESSENTIAL DATA PROTECTION AND PRIVACY CONTROLS

A. DATA PRIVACY

1. The organization shall establish and maintain a clear privacy governance structure with defined roles, responsibilities, and accountability for data protection.
2. Personal data shall only be collected and processed with informed consent where required, supported by clear and transparent privacy notices.
3. Privacy Impact Assessments shall be conducted for new systems, projects, or processes to identify and mitigate potential privacy risks.
4. 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.
5. Data access for Personally Identifiable Information (PII) shall be audited.

B. DATA SECURITY

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

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

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

9. 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.

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

11. 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.

12. 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.

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

C. DATA BREACH

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

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

16. The organization shall ensure timely (72 hrs.), accurate, and transparent communication regarding data breaches to concerned regulators and nCERT.

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

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

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Data Center and Web Hosting Services Controls

NTISB

INTRODUCTION

Pakistan Information Security Framework 2025: **"Essential Data Center and Web Hosting Services Controls"**, outlines the baseline of information security data center controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

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

ESSENTIAL DATA CENTER AND WEB HOSTING SERVICES CONTROLS

A. DATA CENTER

1. The data center's security framework shall encompass robust physical security measures, including access controls, perimeter fencing, video surveillance, visitor management, and other necessary safeguards.

2. Organizations that provide hosting services to entities, or that maintain their own data centers or servers, shall implement and maintain security as follows.

   a) Organizations shall implement network and perimeter security controls, including NGFWs, WAFs, IDS/IPS, DDoS protection, DLP, network segmentation, DMZs, and secure protocols, to safeguard data centers against unauthorized access, malicious activity, and external threats.

   b) Organizations shall implement server hardening practices to reduce attack surfaces and maintain secure configurations, including limiting unnecessary services, disabling unused ports, and enforcing secure protocols.

c) Organizations shall implement and maintain a patch and vulnerability management process to keep systems up to date, address known vulnerabilities, prioritize critical updates, and conduct regular vulnerability assessments.

d) Organizations shall develop, implement, and regularly test Business Continuity and Disaster Recovery Plans to ensure operational continuity during disruptions, in line with organizational requirements and service criticality.

e) Organizations shall deploy monitoring and response solutions, including SIEM, SOAR, and SOC, to detect and mitigate security threats in real time while supporting incident response, threat hunting, and security analytics.

f) Organizations shall implement structured cable management practices, including labelling, separation of power and data cables, and regular inspections, to ensure safety, reliability, and maintainability of data center operations.

g) Organizations shall retain network, system, application, database, and security event logs for a minimum of 12 months and maintain audit trails to ensure comprehensive tracking of system activity.

3. Data centers shall undergo regular internal audits and at least one annual third-party audit.

4. Organizations that do not fulfill the audit requirements shall migrate their services to a secure and compliant data center.

5. Along with the above controls, all data centers shall strictly comply with all relevant and applicable security requirements defined in the nCERT Essential Framework 2025, which encompass 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 audit.

B. EMAIL AND WEB HOSTING SERVICES

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

7. The cybersecurity requirements for protecting the email service shall include at the least the following:

a) Analyze and filter email messages, including phishing emails and spam, using advanced and up-to-date email protection techniques.

b) Implement multi-factor authentication for remote and webmail access to email services.

c) Ensure email archiving and backup to support continuity and compliance.

d) Implement secure management practices and protection mechanisms to defend against Advanced Persistent Threats (APT).

e) Validate their email service domains, by using Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting and Conformance (DMARC) or equivalent measures.

C. WEB APPLICATION SECURITY

8. Organizations shall define, document, approve, and implement cybersecurity requirements for internal and externally accessible web applications, regardless of the hosting environment (on-premises, cloud or third-party services)

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

a. Web applications shall be protected against unauthorized access and malicious activity.

b. Applications shall follow secure architectural principles with layered protection.

c. Secure communication protocols shall be used to protect data in transit.

d. Users shall follow defined secure usage practices.

e. Applications and systems shall be regularly assessed for vulnerabilities.

f. Applications shall be maintained with up-to-date and secure components.

g. Strong authentication mechanisms shall protect externally accessible web applications.

h. Applications shall follow secure development practices and undergo security testing before deployment.

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

11. Organizations shall remain accountable to ensure that requisite security requirements are adequately addressed in contracts and Service Level Agreements (SLAs) with developers and cloud service providers.

PKCERT

Safeguarding Pakistan's Cyberspace

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

National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Critical Information Infrastructure Protection (CIIP) Controls

NTISB

INTRODUCTION

Pakistan Information Security Framework 2025: **"Essential Critical Information Infrastructure Protection (CIIP) Controls"**, outlines the baseline of information security CIIP controls for federal and provincial government ministries and divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

This policy 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.

This policy 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.

ESSENTIAL CIIP CONTROLS

A. GOVERNANCE & RESOURCE ALLOCATION

1. Governance shall be enhanced from the clauses in **"Essential Governance Controls"** and shall be read in conjunction.

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

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

4. 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.

5. A steering committee for cyber security matters shall be formulated and notified headed by the top management of the organization, responsible for making all cyber security related decisions.

6. Cyber security function lead (CISO, CIO, Min. BS-20 or equivalent) shall be part of the steering committee of the organization responsible for all technology related decision making. Cyber security function lead will be directly reporting to the head of the organization.

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

8. The position of cybersecurity function lead, related supervisory and critical positions within the function, must be filled with full-time and requisite experienced cybersecurity professionals.

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

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

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

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

B. CRITICAL ASSET CLASSIFICATION FRAMEWORK

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

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.

Table 1: Critical Asset Classification

14. 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.

Impact on CIA	Non-critical	Critical	Highly Critical	Most Critical
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and sensitive information.	The unauthorized disclosure of information could be expected to have **no**	The unauthorized disclosure of information could be expected to have	The unauthorized disclosure of information could be expected to have **serious**	The unauthorized disclosure of information could be expected to have **severe**

	specific or limited adverse impact on operations, assets or individuals.	**considerable** adverse impact on operations, assets or individuals.	adverse impact on operations, assets or individuals.	**or catastrophic** adverse impact on operations, assets or individuals. (e.g., PII, financials).
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **tolerable or no-specific** adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **considerable, noticeable** adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse impact on operations, assets or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **tolerable or no-specific**	The disruption of access to or use of information or an information system could be expected to have a **considerable/ noticeable** impact on operations,	The disruption of access to or use of information or an information system could be expected to have a **serious** impact on	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** impact on operations,

	impact on operations, assets or individuals.	assets or individuals.	operations, assets or individuals.	assets or individuals. (Unavailability may affect public safety, disruption in a 24/7 service etc.).

Table 2: Asset Classification Based on CIA Impact

Note: ***For convenience or comprehension, organisations 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.***

C. CIA-ALIGNED CONTROL IMPLEMENTATION

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

16. All necessary information security controls including appropriate access control mechanisms according to the criticality of the asset, privileged access controls, authentication, encryption, network security controls, data security and privacy shall be implemented and tested.

17. Data privacy and security shall be maintained, and data retention policies shall be followed to avoid unnecessary retention of sensitive data.

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

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

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

21. Business continuity planning (BCP), Disaster Recovery Plan (DRP) shall be a formal document with clarity of actions, roles and responsibilities, training, drill exercises, proper calculations of the recovery point objective (RPO) (specific to the maximum amount of data that may be lost during a disaster and should be used to guide backup strategies), the maximum tolerable downtime (MTD) and recovery time objective (RTO) (related to the duration of an outage). BCP should be realistic and appropriately approved by the higher management of CII and regulator of the CI sector, wherever applicable.

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

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

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

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

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

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

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

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

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

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

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

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

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Audit Controls

NTISB

Introduction

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

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

Essential Audit Controls

A. CYBER SECURITY AUDIT

1. The organization shall establish an internal audit function with at least annual internal audit. While the oversight/ external audits will be conducted annually by the relevant regulator and NCERT/NTISB, as applicable.

2. 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.

3. The organization shall ensure comprehensive preparation for external and internal audits by defining clear roles, responsibilities, and communication channels, while securing all relevant data and systems prior to auditor engagement.

4. The organization shall mandate that all internal and external cybersecurity audits be performed only by independent, certified, and qualified auditors, selected through defined criteria to ensure credibility, impartiality,

and compliance with regulatory expectations (nCERT registered audit firms should be preferably engaged for consultancy, internal audits and external audits as per the criteria).

5. The organization shall enforce confidentiality agreements (NDAs), and apply technical safeguards such as data masking or watermarking to prevent unauthorized disclosure of sensitive information to auditors.

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

7. The organization shall require every cybersecurity audit to be supported by a documented audit plan, aligned with recognized standards, defining scope, tools, timelines, and resource allocation, and approved by executive management prior to commencement.

8. The organization shall provide all mandatory documentation to the assigned auditor, including but not limited to the Statement of Applicability (SoA), Risk Treatment Plan (RTP), and the duly approved Scope of the Audit signed by the competent authority. These documents shall be accurate, complete, and up to date, ensuring that the audit process is conducted in a transparent, consistent, and effective manner.

9. The organization shall ensure that all audit findings are based on verifiable, sufficient, and securely stored evidence, collected through standardized processes that ensure accuracy, accountability, and audit traceability.

10. The organization shall require all audit observations to be analyzed against defined security baselines, and classified using standardized severity ratings to enable prioritization and risk-based remediation

11. 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.

12. The organization shall mandate a formal closure process for each audit, including confirmation of completed corrective actions, documentation of lessons learned, and integration of findings into organizational risk management practices.

13. The organization shall establish a process of continuous improvement for its audit framework, ensuring alignment with evolving cybersecurity standards, regulatory changes, and emerging threat landscapes.

PKCERT

Safeguarding Pakistan's Cyberspace

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

PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Asset & Risk Management Controls

NTISB

Introduction

Pakistan Information Security Framework 2025: **"Essential Asset & 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.

This document defines the organization's framework for managing assets, software, systems, risks, and cybersecurity 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.

Essential Asset & Risk Management Controls

A. ASSET MANAGEMENT

1. Cybersecurity requirements for managing information and technology assets shall be defined, documented, approved, and implemented.

2. All information and technology assets, including hardware, software, cloud systems, third-party systems, and public-facing services, shall be formally identified, classified, and documented in the official Asset Register, ensuring complete and accurate recording at the time of acquisition.

3. Each asset shall have an assigned owner responsible for its lifecycle management, accurate recordkeeping, and compliance with organizational requirements.

4. 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. Applicable fields are given in Table 1, (organizations may choose the relevant fields):

Table 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, 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 warranty, if applicable)	**Asset Status** (Current operational status, e.g., Active, Inactive, Under Maintenance)	**Confidentiality (0–5)** (How sensitive the information handled by the asset is)	**Integrity (0–5)** (How critical the accuracy of the data handled by the asset is)
Availability (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)

5. Key performance indicators (KPIs) such as maintenance completion, downtime, repair frequency, and Mean Time to Repair (MTTR) shall be tracked and reviewed to evaluate and improve asset maintenance effectiveness.

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

7. Assets shall be securely decommissioned and disposed of at the end of their lifecycle.

8. Complete lifecycle documentation, including acquisition records, usage logs, upgrade details, maintenance history, and disposal certificates, shall be securely maintained and retained for the defined period to support audits, compliance, and accountability.

B. SOFTWARE AND LICENSE MANAGEMENT

9. All licensed software assets shall be properly maintained and updated. Patch management with clear roles and responsibilities shall be ensured.

10. The organization shall enforce a controlled and auditable process for software decommissioning, including valid triggers, stakeholder notification, data retention, and security validation.

11. All licenses and software assets shall be securely retired, reassigned, or disposed of in compliance with financial, regulatory, and information security requirements

C. SYSTEM CATEGORIZATION AND CLASSIFICATION

12. 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.

13. The organization shall assign clear responsibilities for system review and reclassification, including system owners, information security officers, information owners, and compliance/audit teams, ensuring all reclassification activities are accountable, controlled, and auditable.

14. 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.

15. Following categorization and classification can be adopted:

a) Most Critical, Highly Critical, Critical, non-Critical based on severity.

Table 2: Categorization and Classification

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

16. This classification can also be understood while mapping it to confidentiality, integrity and availability (CIA):

Table 3: Unauthorized Disclosure Impact on CIA

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

	could be expected to have a **tolerable or no-specific** impact on operations, assets or individuals.	to have a **considerable/ noticeable** impact on operations, assets or individuals.	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.).

17. However, if the organization is not offering any services, then the classification may also be adopted for confidentiality as follows:

Table 4: Classification Levels

Classification Level	Definition
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.

D. RISK MANAGEMENT

18. The organization shall systematically identify all assets, associated vulnerabilities, and potential threats to establish a comprehensive risk profile.

19. The organization shall evaluate and analyze identified risks by applying defined likelihood and impact criteria, including their effect on confidentiality, integrity, and availability (CIA). Risks shall be assigned quantitative or qualitative values, categorized (e.g., Low, Medium, High, Critical), and recorded in the risk register to enable prioritization for treatment in line with organizational objectives.

20. Essential attributes for risk register shall be recorded, including applicable fields, like the fields given in Table 5 (organizations may choose the relevant fields):

Table 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**

21. The organization shall implement formal risk treatment strategies including mitigation, acceptance, transference, or avoidance assigning clear responsibilities, deadlines, and controls for each risk to ensure residual risks are reduced to acceptable levels.

22. The organization shall continuously monitor risks, 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.).

23. The organization shall establish explicit risk appetite statements for each risk category.

24. The organization shall set measurable risk tolerance thresholds for each risk category.

25. The organization shall assign clear responsibilities for maintaining, monitoring, and enforcing risk appetite and tolerance policies, ensuring transparency, auditability, and alignment with the overall risk management framework.

PKCERT

Safeguarding Pakistan's Cyberspace

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