National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Asset and Risk Management Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Security Framework 2025: **"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 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.

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 store, process, transmit, or protect information and therefore requires security controls to preserve confidentiality, integrity, and availability.

B. 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.

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) must 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.

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 aset)	**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)

10. 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.

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

12. 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.

C. SOFTWARE AND LICENSE MANAGEMENT

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

14. 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.

D. SYSTEM CATEGORIZATION AND CLASSIFICATION

15. 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.

16. Following categorization and classification can be adopted (Table 2):

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.

17. This classification can also be understood while mapping it to confidentiality, integrity and availability (CIA) as given in Table 3.

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

				24/7 service etc.).

18. However, if the organization is not offering any services, then the classification may also be adopted for confidentiality as in Table 4.

19. 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.

20. The asset classification levels are provided in Table 4 for reference.

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.

E. RISK MANAGEMENT

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

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

23. 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.

24. 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**

25. 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.

26. 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.).

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

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

29. The organization shall clearly define risk appetite. Responsibility of risk acceptance shall lie with the risk owner.

PKCERT

Safeguarding Pakistan's Cyberspace

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