



**National Cyber Emergency Response Team**  
Government of Pakistan

# **Pakistan Information Security Framework (PISF) 2026**

## **Essential Asset and Risk Management Controls**



## A. 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.

## 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) 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 1 for reference:

Table 1: Asset Register

Asset Register				
<b>Asset ID</b> (A unique identifier for each asset, e.g., 001, 002)	<b>Asset Name</b> (The name of the asset, e.g., Laptop, Server)	<b>Asset Type</b> (Hardware, Software, etc.)	<b>Expected Life</b> (Anticipated duration before asset becomes obsolete, non-viable, or prone to failure)	<b>Make/Model</b> (Equipment details, e.g., company, model, etc.)
<b>Owner</b> (Responsible for defining requirements, ensuring proper use,	<b>Custodian</b> (Responsible for physical care, day to day maintenance,	<b>Location</b> (Where the asset is physically located, e.g.,	<b>Department</b> (Department using or managing the asset, e.g., IT, HR)	<b>Condition</b> (Current physical condition, e.g.,

and approving disposal)	and documentation)	Office 101, Data Center)		Excellent, Good, Fair)
<b>Disposal Date</b> (Planned or actual date when the asset is no longer in use)	<b>Warranty Status</b> (Expiry date of manufacturer's warranty, if applicable)	<b>Asset Status</b> (Current operational status, e.g., Active, Inactive, Under Maintenance)	<b>Confidentiality (0-5)</b> (How sensitive the information handled by the asset is)	<b>Integrity (0-5)</b> (How critical the accuracy of the data handled by the asset is)
<b>Availability (0-5)</b> (The importance of uptime/accessibility of the asset)	<b>Asset Value w.r.t CIA</b> (Security importance considering Confidentiality, Integrity, Availability)	<b>Security Controls</b> (List security measures implemented, e.g., Antivirus, Firewalls, IDS/IPS)	<b>Classification Level</b> (Sensitivity level based on data handled, business function supported, and potential impact)	<b>Notes</b> (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.

### C. 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.

#### D. 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 2), where Most Critical, Highly Critical, Critical, non-Critical are based on severity.

Table 2: Classification Scheme

Level	Impact of compromise
Most Critical	<b>Catastrophic</b> , can result in extreme safety threats, extreme financial damage, or complete business shut down.
Highly Critical	<b>Severe</b> disruption of essential services, high financial damages etc., safety threats.
Critical	<b>Noticeable</b> operational issues but manageable or medium level financial damages, limited safety threats.
Non-Critical	<b>Minimal</b> 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.

Table 3: Classification mapping with Impact on CIA

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

disclosure, including means for protecting personal privacy and sensitive information.	have <b>no specific or limited</b> adverse impact on operations, assets or individuals.	have <b>considerable</b> adverse impact on operations, assets or individuals.	have <b>serious</b> adverse impact on operations, assets or individuals.	have <b>severe or catastrophic</b> adverse impact on operations, assets or individuals. (e.g., PII, financials).
<b>Integrity</b> 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 <b>tolerable or no-specific</b> adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>considerable, noticeable</b> adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse impact on operations, assets or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse impact on operations, assets or individuals.
<b>Availability</b> 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 <b>tolerable or no-specific</b>	The disruption of access to or use of information or an information system could be expected to have a <b>considerable/noticeable</b> impact on operations,	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> impact on	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> 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.).
--	--	------------------------	------------------------------------	--

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

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

## E. 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 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

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.





## Safeguarding Pakistan's Cyberspace

[info@pkcert.gov.pk](mailto:info@pkcert.gov.pk)  
[www.pkcert.gov.pk](http://www.pkcert.gov.pk)