PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Audit Controls

NTISB

A. INTRODUCTION

1. 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.

2. This framework 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.

B. CYBER SECURITY AUDIT

3. The organization shall establish an internal audit function with at least annual internal audit. While the oversight/ external audits may be conducted by the relevant regulator and nCERT/NTISB as applicable.

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

5. The organization shall mandate that all internal and external cybersecurity audits be performed only by independent, certified, and qualified auditors, selected through defined criteria to ensure credibility, impartiality, and compliance with regulatory expectations (audit firms, registered with nCERT/ sectoral CERTs/ relevant regulator, should be preferably engaged for consultancy, internal audits and external audits as per the criteria).

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

7. 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.

8. 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.

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

10. 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.

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