National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

Essential Audit Controls

A. INTRODUCTION

1. Pakistan Information Security Framework: **"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 information security audits, in alignment with regulatory requirements and organizational objectives. Aim is to strengthen governance through independent information security audits and continuous improvement.

B. INFORMATION SECURITY AUDIT

3. The organization shall establish an independent internal audit function responsible for information security audits, with audits conducted at least annually. While the oversight/external audits may be conducted by the relevant regulator and nCERT/NTISB as applicable.

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

5. The organization shall mandate that all internal and external information security audits are conducted by independent, certified, and qualified auditors, selected through formally defined criteria.

6. Audit firms, registered with nCERT/ sectoral CERTs/ relevant regulator, should be preferably engaged for consultancy, internal audits and external audits as per the criteria.

7. The organization shall enforce confidentiality obligations, including Non-disclosure agreements (NDAs), least-privilege access controls, and apply technical safeguards such as data masking or watermarking, acknowledging audit data sensitivity.

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

9. The organization shall require every information security audit to be supported by a documented and approved audit plan, aligned with recognized standards, defining scope, objectives, tools, timelines, and resource allocation.

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

11. The organization shall ensure that all audit findings are supported by verifiable, sufficient, and securely stored evidence, collected and retained through standardized processes that ensure integrity, traceability and accountability.

12. The organization shall ensure that audit results are documented in a standardized report format, communicated to relevant stakeholders, and retained in compliance with regulatory requirements and organizational policies.

13. The organization shall enforce a formal closure and follow-up process for each audit, including confirmation of completed corrective actions, validation of remediation effectiveness, documented risk acceptance where applicable, escalation of overdue actions, documentation of lessons learned, and integration of findings into organizational risk management practices.

14. The organization shall establish a process of periodic review and continuous improvement for its audit framework, ensuring alignment with evolving information security standards, regulatory changes, organizational objectives, and emerging threat landscapes.

PKCERT

Safeguarding Pakistan's Cyberspace

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