National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Supply Chain Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework: **"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.

2. This framework 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.

B. SUPPLY CHAIN CONTROLS

3. The organizations shall define, document, approve and implement policies, procedures, and processes for managing supply chain risks for products, systems, and services provided by third parties.

4. The organization shall identify, assess and classify supply chain risks across defined categories with special emphasis on information security, third-party access, operational dependency and critical supplier dependencies.

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

6. All identified supply chain risks shall be continuously monitored, tracked, and reviewed at defined intervals or upon significant changes, to ensure timely response, escalation and remediation.

7. Organizations procuring services like cloud services, Data Centers, Web hosting, Secure software development, etc. must ensure that the service providers comply with relevant policy frameworks in the PISF and/or applicable laws, regulations and sector specific policies

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

9. The organization shall conduct risk-based due diligence on all suppliers prior to engagement to ensure compliance with applicable security, legal, and regulatory requirements.

10. All supplier agreements and Service Level Agreements (SLAs) shall include contractual provisions covering information security, data protection, confidentiality, audit rights, incident notification timelines, and compliance obligations.

11. The organization shall be accountable for all the risk accepted by any third party, which can have significant impact on the organization.

12. The organization shall ensure transparency and verification of supplier source, including the origin, authenticity and integrity of products, services, software components, data and evaluate risks related to acquiring products or services from hostile jurisdictions.

13. Organizations shall ensure that suppliers handle, process, store, and share organizational data strictly in accordance with approved security and privacy requirements (Ref: Data protection and privacy policy).

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

15. Organizations shall ensure that suppliers detect, report, and coordinate with the organization on security incidents affecting data or services, in accordance with defined procedures, notification timelines, and joint incident response mechanisms.

16. Organizations shall ensure that suppliers maintain documented and tested business continuity and disaster recovery capabilities appropriate to ensure resilience of critical services.

17. Organizations shall ensure that the suppliers remain fully accountable for the actions of their subcontractors and fourth parties.

18. Organizations shall ensure secure off-boarding of supplier, including returning or securely destroying data, revoking access, undergoing exit audits, and ensuring service continuity and data integrity upon contract completion/ Termination.

19. Significant changes in supplier scope, ownership, location, or service delivery shall trigger a reassessment of supply chain risks.

20. The organization shall identify and manage concentration risks arising from single-source or highly dependent suppliers.

21. Relevant personnel involved in procurement and supplier management shall receive periodic training on supply chain risk management requirements.

PKCERT

Safeguarding Pakistan's Cyberspace

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