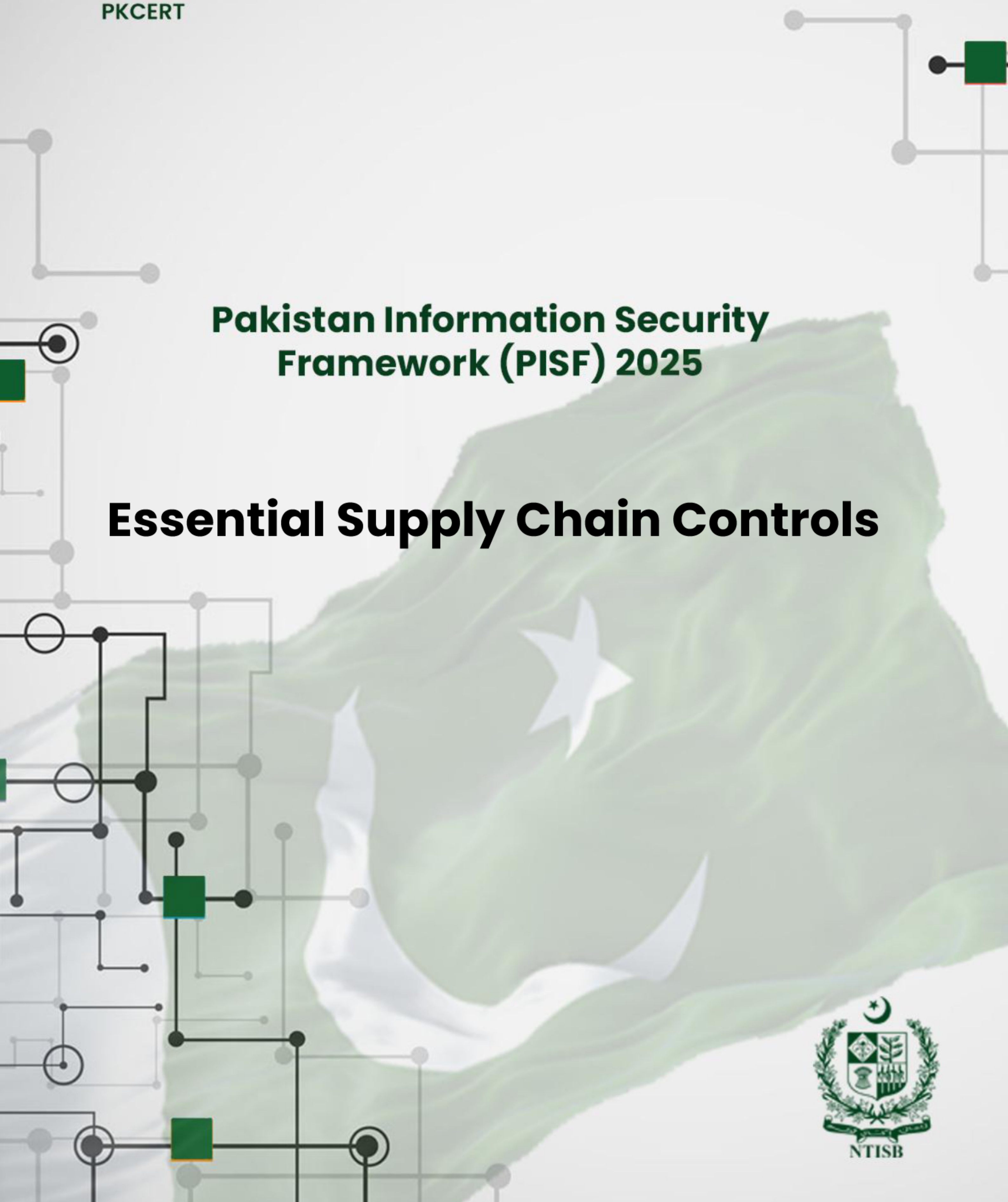
PKCERT

National Cyber Emergency Response Team
Government of Pakistan



Pakistan Information Security Framework (PISF) 2025

Essential Supply Chain Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework 2025: **"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 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 and classify supply chain risks across defined categories with special emphasis on cybersecurity, third-party access, and critical supplier dependencies.

5. The organization shall implement risk-specific mitigation strategies, including supplier diversification, contingency planning, cybersecurity 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 to ensure timely response and remediation.

7. Organizations procuring services like cloud, Data Center, Web hosting, Secure software development etc. must ensure that the service providers comply with relevant policy frameworks in the PISF 2025 and/or applicable laws/ regulations (e.g cloud policy).

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

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

10. All supplier agreements and Service Level Agreements (SLAs) must include contractual provisions addressing information security, data protection, confidentiality and compliance obligations.

11. The organization shall ensure transparency and verification of supplier source, including the origin and integrity of products, services, and data.

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

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

14. Organizations shall ensure that suppliers detect, report, and coordinate with the organization on security incidents affecting data or services, following defined procedures, timelines, and joint response mechanisms.

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

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

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

PKCERT

Safeguarding Pakistan’s Cyberspace

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