National Cyber Emergency Response Team

Engagement and Oversight Framework by nCERT for Compliance and Audit Activities of Registered Firms

Introduction and Purpose

The Pakistan Information Security Framework (PISF), developed under the National Cyber Emergency Response Team (nCERT), establishes standardized policies, security controls, and compliance mechanisms to safeguard national information systems and critical infrastructure.

Pursuant to PISF 2026, CERT Rules 2023, Chapter III, Clause 12(c), and Objective III of the PKCERT PC-I, which mandate nCERT to conduct periodic security audits and infrastructure assessments, nCERT has developed the Framework for the Engagement and Oversight of Registered Firms.

For the purposes of audits and compliance consultancies conducted under this mandate, only the firms duly registered with nCERT shall be eligible for engagement. This Framework formally establishes the activity oversight mechanisms governing the engagement of registered firms by organizations subject to the requirements, thereby ensuring consistency, transparency, accountability, and compliance with applicable Pakistan Information Security Framework (PISF) requirements.

This document deals with the activities related to IT and OT domains. While mechanism for audits/assessments related to the domain of Cloud will be according to the Cloud First Policy governed by Cloud office of MoITT.

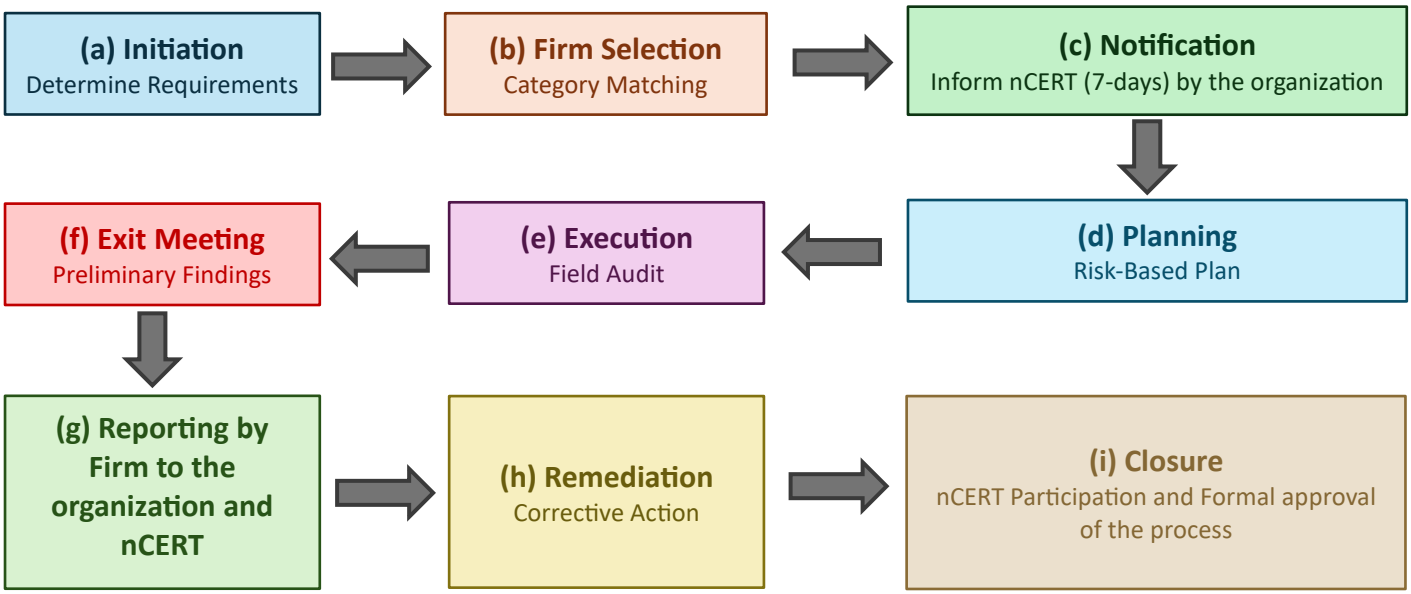
Scope and Applicability

This Framework shall be applicable to all government organizations, including federal and provincial government ministries, divisions, departments, autonomous bodies, public sector corporations and designated Critical Information Infrastructure (CII) entities. It shall further apply to all firms duly registered with nCERT and engaged to undertake compliance readiness/ gap assessments/audits of such organizations for evaluating compliance with the Pakistan Information Security Framework (PISF).

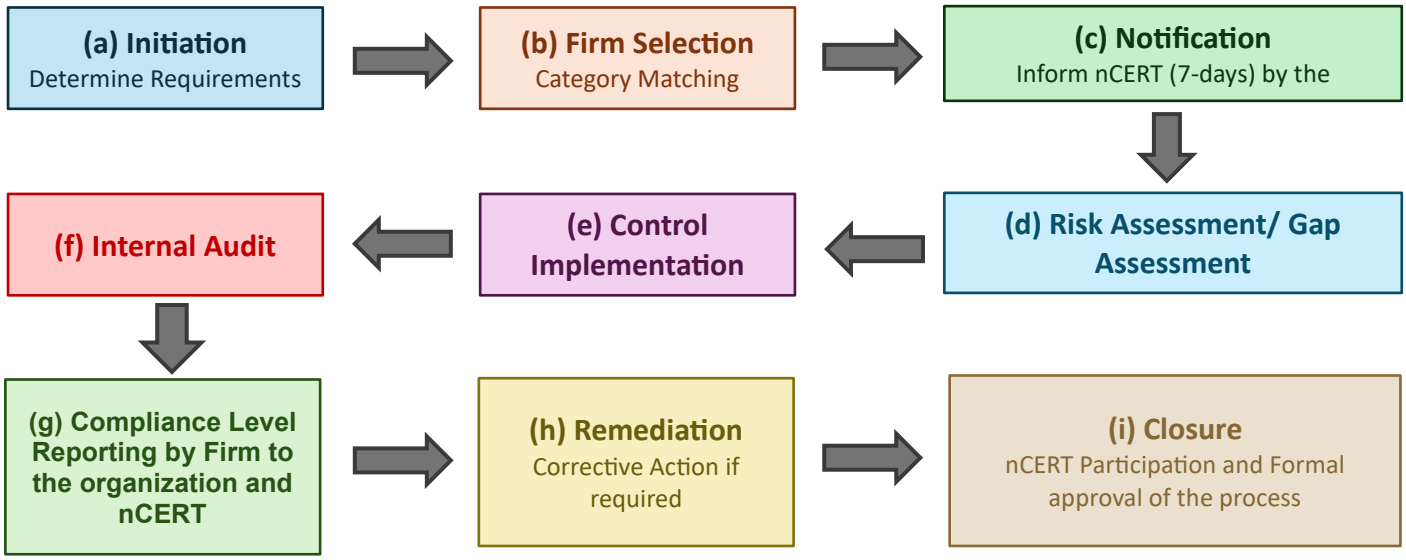
Registered Firm Engagement Process

The engagement by any Government organization for the registered firms shall be conducted through the following processes for Audits and Compliance Readiness engagements:

Audit Process



Compliance Readiness Consultancy Process



a) Initiation of the Engagement

The Organization shall determine its requirements in accordance with PISF and identify the applicable scope, including information technology, operational technology (OT) environments, cloud infrastructure, and other supporting assets.

b) Selection of the Registered Firm

The Organization shall engage the firm duly registered with nCERT and holding the appropriate category of registration, according to the following classification criteria:

Organization Code	Organization Type	Scope	Audit Firm (To be Selected)
A	Critical Sectors	Highest Security Requirements, IT/OT/Cloud (More than 150 Nodes)	CAT-I
B	Critical Sectors	Enhanced Security, IT/OT/Cloud (Up to 150 Nodes)	CAT-II, CAT-I
C	Non-Critical Sectors	Intermediate Security, IT Only (More than 150 Nodes)	CAT-III,CAT-II, CAT-I
D	Non-Critical Sectors	Intermediate Security, IT Only (Up to 150 Nodes)	CAT-IV,CAT-III, CAT-II, CAT-I

The updated list of registered firms is maintained by nCERT and published on its official website at https://pkcert.gov.pk/registered-firms.asp.

Selected firm will sign the Non-Disclosure Agreement (NDA) with the organization and will safeguard the confidentiality of all the information they access during the whole engagements. All team members of the firm will also sign the NDA.

Team Composition:

The selected firm shall deploy suitably qualified and experienced personnel to conduct the assigned activity in accordance with the following minimum criteria.

Organization Code	Organization Type	Human Resource Engagement		
		Expert	Senior	Junior
A	Critical Sectors	1	2	4
B	Critical Sectors	1	1	3
C	Non-Critical Sectors	0	1	2
D	Non-Critical Sectors	0	1	2

The qualification and experience requirements for Expert, Senior, and Junior auditors are prescribed by nCERT and published on its official website at https://pkcert.gov.pk/consultant-registration.asp.

Conflict of Interest Requirements

Following scenarios shall be considered as conflict of interest:

i) A firm which has provided consultancy or implementation services related to the controls cannot be engaged for the audit of the same organization.
ii) Any member of the team formulated by the firm has a direct financial, managerial, or employment relationship with the Organization;
iii) Any circumstance exists that may impair firm's independence, objectivity, or professional judgment.
iv) The firms shall submit a formal Conflict-of-Interest Declaration to both the Organization and nCERT prior to commencement of the assigned activity.

c) Notification to nCERT

Within seven (07) working days of engagement, the selected firm shall formally notify nCERT of the engagement and provide:

i) Name of the Organization
ii) Scope and objectives of the engagement
iii) Proposed activity timeline
iv) Composition of the team
v) Declaration of independence and absence of conflict of interest

d) Activity Planning

The firm shall prepare a risk-based plan of the activity, including methodology, sampling approach, evidence collection procedures, and reporting mechanisms. The activity/audit plan shall be made available to nCERT upon requirement.

e) Task Execution

The firm shall conduct the activity in accordance with PISF requirements or regulatory applicable standards, and professional auditing practices. All findings shall be supported by sufficient and verifiable evidences.

f) Audit Exit Meeting

Upon completion of field activities, the firm shall conduct a closing meeting with the Organization to communicate preliminary findings, observations, non-conformities, and recommendations.

g) Submission of the Final Report

Audit report/Internal Audit Report/Risk assessment Report or any other relevant documents or information pertaining to the activity, shall be submitted to the organization by the Firm and the same will be shared with nCERT.

h) Corrective Action and Remediation

The Organization shall prepare and implement a corrective action plan for identified non-conformities and provide progress updates as required by nCERT.

i) Activity Closure

The Process shall be deemed closed only after acceptance of the report by nCERT and completion of any required follow-up activities.

nCERT Oversight and Governance

nCERT, NTISB and Sector regulator or authorities shall serve as the oversight entities for all activities conducted under the Pakistan Information Security Framework (PISF). They reserves the right to:

i) Review notifications, plans, reports, and supporting documentation
ii) Conduct quality assurance reviews of completed tasks
iii) Participate in opening meetings, technical review sessions, and closing meetings;
iv) Observe activities on-site or remotely
v) Require registered firms to provide working papers, sampling records, evidence repositories, and assessment documentation.
vi) Conduct shadow audits, witness audits, or independent validation assessments
vii) Perform full or partial re-assessments of audited organizations
viii) Verify the competence and deployment of team members
ix) The relevant authority will investigate complaints, disputes, or allegations of audit or misconduct
x) Suspend, downgrade, or revoke the registration of audit firms that fail to comply with nCERT requirements.

Quality Assurance and Enforcement

Where material deficiencies, negligence, misrepresentation, or professional misconduct are identified, nCERT may impose one or more of the following measures:

a) Issuance of corrective action notices
b) Mandatory re-audit at the audit firm's expense
c) Temporary suspension from the nCERT audit registry
d) Downgrading of audit firm category
e) Permanent removal from the nCERT registry

The decisions of nCERT regarding audit oversight, quality assurance, and enforcement actions shall be final and binding for the purposes of this Framework.

Note: *nCERT reserves the right to levy fees for oversight activities conducted under this Framework, and such charges shall be prescribed and implemented in future in accordance with applicable rules and regulations.*