# National Cyber Emergency Response Team

## Criteria for Cyber Security Auditing & Compliance Firm's Registration

### Scope

Registration criteria of cyber security auditing & compliance firms with nCERT for conduct of comprehensive cyber security audits of IT/Cloud/OT to ensure compliance with established information security standards, frameworks and policies like Pakistan Cloud First Policy, Pakistan Information Security Framework (PISF) and to conduct consultancy services for audit readiness against PISF.

### Description

This criterion pertains to firms seeking registration as cyber security auditing & Compliance firm with the nCERT. These firms will conduct a range of essential cyber security audit, compliance readiness and assessment activities of IT/Cloud/OT infrastructure in Pakistan. Service Providers, providing a range of services including but not limited to IT services, hosting, cloud, Security or managing/offering infrastructure to provide such services will be able to opt for their service/infrastructure audit from the approved auditing & compliance firms.

Registered Firms can be engaged by public sector organizations, as per their regulations, policies and procedures to conduct:

a. Cyber Security Audit & Compliance of CSP as per the criteria laid down by Pakistan Cloud First Policy.

b. Cyber Security Audit & Compliance of organizations against the established standards and PISF.

c. Consultancy for Audit readiness, Gap assessment and services related to PISF implementation.

**This should be noted, that any firm engaged for consultancy in the design, development, implementation, or maintenance of cybersecurity controls, systems, or solutions for an auditee shall not be eligible for conducting audit for the same organization**.

To qualify for registration, firms must adopt methodologies and practices aligned with established standards for information security and industry best practices. This registration process is essential to ensure the competency of firms tasked with auditing IT/Cloud/OT infrastructure. The outlined criteria emphasize the requirements and expectations for firms seeking registration to perform cyber security assessments, highlighting the importance of adhering to established standards and protocols, ensuring the integrity and effectiveness of IT/Cloud/OT infrastructure within Pakistan's cyber landscape.

## A. General Rules for Cyber Security Audit Firms

| | |
|---|---|
| 1. | The cyber security audit & compliance firm must be registered with SECP or the Registrar of firms. Additionally, the company/firm should appear on the Active Taxpayer list (ATL) of income and sales tax issued by FBR. |
| 2. | Any auditee shall not engage any audit firm which has been previously involved as a subsidiary, affiliate, or associate firm of the auditee to avoid conflicts of interest. An affidavit declaring this claim must be submitted before conducting the audit. |
| 3. | The cyber security audit & compliance firm should refrain from outsourcing its cyber security audit, compliance, penetration testing, and red teaming engagements to any foreign third-party assessor, auditor, or audit & compliance firm. |
| 4. | Foreign companies with local branch offices in Pakistan are eligible to apply, provided they are registered with SECP, or the registrar of firms in Pakistan. |
| 5. | Firms must have clear understanding of National policies, procedures and standards related to IT, IT Security, Cyber Security and data protection aspects etc. that are published on Govt websites including MoITT, PTA, nCERT and NTISB. Few such documents include National Cyber Security Policy, Pakistan Cloud First Policy, Accreditation Criteria of Cloud Service Providers, Pakistan Security Standard for Evaluation of Cryptographic and IT Security Devices, Data Protection Bill (draft), Pakistan Information Security Framework (PISF) by nCERT etc. |
| 6. | Cyber security audit & compliance Firm should not be a blacklisted entity in the Public or Private sector within Pakistan or abroad, due to any factor including but not limited to unsatisfactory performance, breach of general/specific instructions or NDA, corrupt practices and/or any fraudulent activity. |
| 7. | Cyber security audit & compliance firms can perform audits & compliance activities within their respective categories or downward in the hierarchy as outlined in Section-D. For example, firms qualifying for CAT-I can also conduct audits & compliance activities of Service Providers or organizations falling under CAT-II to CAT-IV. Similarly, firms qualifying for CAT-II can audit CAT-III and CAT-IV Service Providers. However, firms qualifying for Cat-IV cannot conduct audits of Service Providers higher in the hierarchy, i.e., CAT-III to CAT-I. |
| 8. | Cyber security audit & compliance firm must perform onsite audits by ensuring a detailed review of security measures, processes, and compliance with standards, while identifying weaknesses. |
| 9. | When assessing the cyber security audit & compliance firm, nCERT may review several key areas of discipline, including but not limited to:<br>▪ Assessment methodology<br>▪ Profiles of certified individuals/resources |

| | |
|---|---|
| | ▪ Data storage and retention policies<br>▪ Information sharing policy and procedure<br>▪ Tools and reporting methodology<br>▪ Experience of Conduct of similar audits<br>▪ Sample Audit reports |
| 10. | nCERT reserves the right to conduct a full assessment at any given point in time. This assessment may require re-submission of all relevant documents submitted at the time of registration or any additional documents necessary for further scrutiny. |
| 11. | In the event of a violation of any clause of the NDA by an approved cybersecurity audit & compliance firm, and where such violation is duly proven or established, the relevant information and supporting details may be provided to nCERT. Upon such determination, nCERT reserves the right to terminate the registration of the concerned cybersecurity audit & compliance firm. In case of termination, the information shall be duly updated on the nCERT website. |
| 12. | List of approved cyber security Audit & Compliance firms will be published on the website of nCERT and regularly updated. |
| 13. | nCERT reserves the right to revise cyber security Audit & Compliance firm registration criteria as and when needed. Revision criteria will be communicated to registered firms as well as published on nCERT website. |
| 14. | Registration may be revoked in the event of any legal or criminal offense. |
| 15. | Organization should implement a quality management system based on ISO 9001 or relevant standard. |
| 16. | For firms currently or previously affiliated with the public sector, experience in auditing critical infrastructure (IT/OT) will be considered on a commensurate basis for firm categorization if provided with appropriate/ verifiable evidence. |
| 17. | Accreditation of audit and compliance firms will be renewed every 2x years. |
| 18. | The firm must provide **project completion certificates** with clearly mentioned client's name, project scope, and completion date. |
| 19. | The firm must provide at least three client references or a list of previous clients to validate their credibility. |
| 20. | Details and requirements for firm registration are provided in the following tables. (i.e Table B,C,D,E) |

## B. Category Classification

| Category | Organization Type | Scope |
|---|---|---|
| CAT-I | Critical Sectors | Highest security requirements IT/OT/Cloud security (More than 150 nodes) |
| CAT-II | Critical Sectors | Enhanced security IT/OT/Cloud security (Up to 150 nodes) |
| CAT-III | Non-Critical Sectors | Intermediate security IT only (More than 150 nodes) |
| CAT-IV | Non-Critical Sectors | Baseline security IT Services only (Up to 150 nodes) |

**Note:** All sectors/organizations designated as Critical shall fall into CAT-I and CAT-II categories, while those not included in Critical shall be categorized as CAT-III and CAT-IV.

## C. Required Standards by Category

A firm can qualify in specific category for one or more than one domain: IT Security, Cloud Security and OT Security. The organizations while engaging firms will have to select appropriate firm in the relevant category and in the specific domain.

| Category | IT Security Standards | CSP Audits as per Cloud First Policy ISO 17021 accreditation (mandatory) | OT Security Standards |
|---|---|---|---|
| **CAT-I** | ISO/IEC 27001: 2022 | ISO/IEC 27001: 2022 or equivalent<br>Where applicable<br>• ISO/IEC 27005:2022 or equivalent<br>• ISO/IEC 27017:2015 or equivalent<br>• ISO/IEC 27070:2021 or equivalent<br>• Sector specific e.g. PCI DSS, HIPAA or equivalent<br>• CSA STAR Certification or equivalent<br>• SOC2 (Managing Customer Data) or equivalent<br>• Relevant Sector Specific Standards | ISO/IEC 27001: 2022 + Experts with ISA/IEC 62443 Cybersecurity Risk Assessment Specialist Certificate. |

| | | | |
|---|---|---|---|
| **CAT-II** | ISO/IEC 27001: 2022 | ISO/IEC 27001: 2022 + ISO/IEC 27005:2022 or equivalent Where applicable<br>ISO/IEC 27017:2015 or equivalent | |
| **CAT-III** | ISO/IEC 27001: 2022 | ISO/IEC 27001: 2022 +<br>Where applicable ISO/IEC 27017:2015 | ISO/IEC 27001: 2022+ Experts with Cybersecurity fundamentals Specialist Certificate |
| **CAT-IV** | ISO/IEC 27001: 2022 | ISO/IEC 27001:2022 | ISO/IEC 27001: 2022 |

## D. HR Requirements by Category

| Category | Expert Level | Senior Level | Junior Level | Total HR Equivalent |
|---|---|---|---|---|
| **CAT-I** | 1 | 2 | 4 | 10 technical resources (6 certified) |
| **CAT-II** | 1 | 1 | 3 | 8 technical resources (4 certified) |
| **CAT-III** | 0 | 1 | 2 | 6 technical resources (4 certified) |
| **CAT-IV** | 0 | 1 | 2 | 4 technical resources (2 certified) |

***Note:*** *Expert, Senior, and Junior levels can be referred as in the* ***Consultant Levels Criteria*** *published by nCERT or equivalent.*

## E. Firm Work Experience Requirements

| Category | CSP Audits as per Cloud First Policy | PISF Compliance Readiness / Audit for IT Infrastructure | Compliance Readiness / Audit for OT Infrastructure |
|---|---|---|---|
| **CAT-I** | **Min Experience:** 8 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **20 audits & compliance readiness activities** across at least **3 different sectors** or international standards including Cloud Security standards. | **Min Experience:** 6 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **15 audits & compliance readiness activities** across a minimum of **2 different sectors** or international standards, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against no fewer than two different standards. | **Min Experience:** 6 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **15 audits & compliance readiness activities** across a minimum of **2 different sectors** or international standards, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against no fewer than two different standards, with one specific to OT security. |
| **CAT-II** | **Min Experience:** 5 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **15 audits & compliance readiness activities** across at least **2 different sectors** or international standards including Cloud Security standards. | **Min Experience:** 4 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **12 audits & compliance readiness activities** across a minimum of **2 different sectors** or international standards, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against no fewer than two different standards. | **Min Experience:** 4 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **12 audits & compliance readiness activities** across a minimum of **2 different sectors** or international standards, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against no fewer than two different standards, with one specific to OT security. |
| **CAT-III** | **Min Experience:** 5 years **Audit & Compliance Readiness activities Experience:** The firm must have experience of conducting a minimum of **8 audits & compliance readiness activities** in any **one sector** or international standard, preferably | **Min Experience:** 3 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **8 audits & compliance readiness activities** across any one sector or international standard, or alternatively, possess equivalent | **Min Experience:** 3 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **8 audits & compliance readiness activities** across any one sector or international standard, or alternatively, possess equivalent |

| | | | |
|---|---|---|---|
| | including Cloud Security standards. | experience in providing consultancy services for audit readiness against **any one standard**. | experience in providing consultancy services for audit readiness against **any one standard** specific to OT security. |
| **CAT-IV** | **Min Experience:** 3 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **5 audits & compliance readiness activities** in any **one sector** or international standard, preferably including Cloud Security standards. | **Min Experience:** 3 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **5 audits & compliance readiness activities** across any **one sector** or international standard, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against **any one standard**. | **Min Experience:** 3 years **Audit & Compliance Readiness Experience:** The firm must have experience of conducting a minimum of **5 audits & compliance readiness activities** across any one sector or international standard, or alternatively, possess equivalent experience in providing consultancy services for audit readiness against **any one standard** specific to OT security. |

**Note:** Based on the potential and/or performance of an audit & compliance firm, nCERT may grant a relaxation of up to 2 years in experience to the firm in each category during the selection assessment process or after selection (during the accreditation/licensing period).