General Rules for Registration of Audit Companies/Firms

1. All registered audit companies/firms shall ensure that **each audit report is signed by qualified/certified professionals** as follows: -

   a) **Category 1:** Signed by **four (04) professionals**, with their names and qualification(s)/certification(s). At least one (01) expert from each of the following areas: GRC, SOC, PenTest, **and** Lead Auditor.
   b) **Category 2:** Signed by **four (04) professionals**, with their names and qualification(s)/certification(s). At least one (01) expert from each of the following areas: GRC, SOC, PenTest, **and** Lead Auditor.
   c) **Category 3:** Signed by **three (03) professionals**, with their names and qualification(s)/certification(s). At least one (02) expert from GRC, SOC or PenTest, **and one (01)** Lead Auditor.
   d) **Category 4:** Signed by **two (02) professionals**, with their names and qualification(s)/certification(s). At least one (01) expert from GRC, SOC or PenTest, **and one (01)** Lead Auditor.

2. The audit company/firm **shall deliver clear, actionable audit reports containing findings, risk ratings, and remediation roadmaps**, and shall conduct follow-up audits to verify closure of identified issues.
3. The audit company/firm **must possess the capability to audit across IT and telecom infrastructures/ systems**, including networks, applications, cloud, physical security, and operational technology (OT), and may be capable of performing penetration testing, vulnerability assessments, configuration reviews, and architectural reviews.
4. All **audits must be conducted onsite**. Virtual or online audits shall not be permitted under any circumstances.
5. Registered audit companies/firms must adhere to information security best practices and maintain documented policies and procedures.
6. Registered audit companies/firms will conduct audits for their designated category and/ or any lower category as specified on PTA's Website.
7. The audit company/firm **must not have any conflict of interest with the entity being audited**.
8. The company or firm, including any of its partners or auditors, must not have been involved in, or subjected to, any disciplinary proceedings or regulatory penalties arising from matters related to audit performance, professional misconduct, or data handling practices.

9. In case of **any change in technical resource(s), the registered audit company/firm shall notify the Cyber Security Directorate of any outgoing and incoming technical resource(s), along with their General Police Verification** or Police Character Certificate where applicable, through the company's letterhead duly signed by the Chief Executive Officer (CEO). This notification must be submitted within 30 days of any such change.
10. Registered audit companies/firms must not be blacklisted by any public or private sector organization in Pakistan or abroad.
11. Registered **audit companies/firms must sign a Non-Disclosure Agreement (NDA) with the auditee licensee prior to commencement of the audit**. The NDA must include, but is not limited to: purpose and scope, definition of confidential information, obligations of the audit company/firm, **duration of confidentiality, exceptions, breach consequences, return or destruction of information, non-solicitation and conflict of interest, and dispute resolution**.
12. Registered audit **companies /firms are required to submit to PTA a list of audits conducted during each year**, along with a satisfactory Project/Audit Closure Certificate issued by the respective licensee for each audit.
13. PTA reserves the right to conduct a full assessment of any registered audit company/firm at any time.
14. PTA may review key aspects such as assessment methodology, profiles of certified individuals, data storage and retention policies, information-sharing protocols, tools, and reporting methodologies.
15. Each **registered audit company/firm shall undergo a review process every three (03) years**. Review of registration shall be subject to evaluation of the firm's previous audit reports, if any.
16. In the **event of any deficiency, professional negligence, or submission of a poor-quality audit report by a registered auditor, PTA reserves the right, re-evaluate the firm's category or de-list it**.
17. PTA shall maintain and regularly update a public list of registered information security audit companies/firms on its website.
18. **PTA reserves the right to modify the registration criteria or process at any time without prior notice**. In the event of any revisions, companies or firms must submit a new application in accordance with the updated criteria.