

**आईआरडीएआई के साइबर सुरक्षा दिशानिर्देशों के तहत
लेखापरीक्षक अथवा लेखापरीक्षण फर्म की नियुक्ति की शर्तें**

1. क. उक्त सनदी लेखाकार फर्म को एक पार्टनरशिप फर्म / लिमिटेड लायबिलिटी पार्टनरशिप अधिनियम, 2008 के तहत लिमिटेड लायबिलिटी पार्टनरशिप (एलएलपी) फर्म होना होगा, जो कि इंस्टिट्यूट ऑफ चार्टर्ड अकाउंटेंट्स ऑफ इंडिया (आईसीएआई) में पंजीकृत हो, व निम्नलिखित मानदंडों को पूरा करते हों :

- क. कम से कम पाँच वर्षों का निरंतर कार्य (प्रैक्टिस) होनी चाहिए।
- ख. नियुक्ति की तिथि से पूर्व कम से कम चार साझेदार होने चाहिए।
- i. कम से कम एक साझेदार को आईसीएआई द्वारा सर्टिफायड इन्फॉर्मेशन सिस्टम्स ऑडिटर (सीआईएसए) / डीआईएसए होना चाहिए।
- ii. कम से कम एक साझेदार को आईसीएआई का फेलो सदस्य होना चाहिए।
- iii. कम से कम एक साझेदार के पास, या तो बीमा कम्पनियों अथवा बैंकों अथवा म्युचुअल फंडों की साइबर सुरक्षा/सूचना सुरक्षा समीक्षा अथवा साइबर सुरक्षा / सूचना सुरक्षा लेखापरीक्षा करने का कम से कम तीन वर्षों का अनुभव होना चाहिए।
- iv. कम से कम एक साझेदार के पास, आईटी वातावरण में लेखापरीक्षा करने एवं दूरस्थ स्थान से लेखापरीक्षा करने का अनुभव होना चाहिए।

अथवा

ख. सर्ट - इन सूचीबद्ध बाह्य प्रणाली लेखापरीक्षक, जो सीआईएसए / डीआईएसए द्वारा प्रमाणीकृत हों।

2. लेखापरीक्षक अथवा लेखापरीक्षण फर्म अथवा इसके कोई भी साझेदार को, कभी भी किसी भ्रष्टाचार अथवा धोखाधड़ी के लिए भारत सरकार अथवा किसी राज्य सरकार अथवा आईआरडीएआई अथवा सेबी अथवा आरबीआई अथवा आईसीएआई अथवा सर्ट-इन अथवा एसएफआईओ अथवा किसी विनियामक द्वारा प्रतिबंधित अथवा अयोग्य घोषित नहीं होना चाहिए तथा उनके खिलाफ कोई अनुशासनात्मक कार्रवाई बकाया नहीं होनी चाहिए।
3. आईआरडीएआई साइबर सुरक्षा दिशानिर्देशों के तहत प्रमाणीकरण में प्रबंधन द्वारा प्रतिनिधित्व (एमआर) अथवा अन्य लेखापरीक्षकों के कार्य पर विश्वास करना मान्य नहीं होता है, क्योंकि लेखापरीक्षक को उन विनियामक संस्थाओं द्वारा नियुक्त किया जाता है, जिन्हें आईआरडीएआई के आदेशानुसार पॉलिसीधारकों एवं सामान्य सार्वजनिक सूचना / डाटा की सुरक्षा करनी चाहिए। अतः, लेखापरीक्षक अपना लेखापरीक्षण का कार्य मान्य मानदंडों के अनुसार साक्षात्कारों, दस्तावेज सत्यापन, अनुपालन जाँच, नियंत्रणों की पर्याप्त जाँच द्वारा करेगा।

4. लेखापरीक्षक, प्रमाणीकरण कार्य करने के दौरान, उन सभी कार्य नोटों, अभिलेखों का रख-रखाव करेगा जो आवश्यकतानुसार प्राधिकरण को प्रदान किए जा सकते हैं।
5. विनियमित संस्था द्वारा, नियोजन-पत्र को जारी से पूर्व, लेखापरीक्षक से उपरोक्त शर्तों की पूर्ति किए जाने संबंधित घोषणा प्राप्त करनी होगी तथा लेखापरीक्षक से संबंधित विवरणों को नियोजन - पत्र की एक प्रति के साथ रखना होगा, जो कि आवश्यकतानुसार प्राधिकरण को प्रदान की जा सकती है।

APPOINTMENT OF AUDITOR OR AUDIT FIRM UNDER

1. **A.** The Chartered Accountant firm shall be a Partnership Firm / Limited Liability Partnership (LLP) firm under the Limited Liability Partnership Act, 2008, registered with the Institute of Chartered Accountants of India (ICAI), who fulfil the following criteria:
 - a. continuous practice of at least five years
 - b. a minimum of four partners before the date of appointment
 - i. at least one Partner shall be Certified Information Systems Auditor (CISA) / DISA of ICAI.
 - ii. at least one partner shall be a Fellow Member of the ICAI,
 - iii. at least one Partner shall have a minimum of three years of experience in Cyber Security / Information Security review or Cyber Security / Information Security audit of either Insurance Companies or Banks or Mutual Funds
 - iv. at least one partner has the experience of audit in IT environment and in conducting Audit from remote location

OR

- B.** Cert-in empanelled external systems Auditor holding CISA / DISA certifications.
2. The auditor or audit firm or any of its partners should not have been banned or declared ineligible for corrupt and fraudulent practices by the Government of India or any State Government or IRDAI or SEBI or RBI or ICAI or Cert-In or SFIO or any regulator **and** should not have any pending disciplinary proceedings.
 3. The certification under IRDAI Cyber Security Guidelines does not recognise Management Representations (MRs) or reliance on other auditors' work, as the Auditor is engaged by Regulated Entities who are to protect Policyholders and General Public information / data, as a part of IRDAI's mandate. Thus, the Auditor shall perform the Audit with interview, document verification, compliance checks, substantive checks of controls as per recognised standards.
 4. The Auditor, in undertaking the Certification work, shall maintain all working notes, records which may be provided to the Authority when required.
 5. The Regulated Entity shall, before issuing the engagement letter, obtain relevant declaration, from the auditor in compliance of the above conditions and maintain the details of the Auditor along with a copy of the engagement letter which may be provided to the Authority when required.