Telangana State Co-operative Apex Bank Ltd.
(State Govt. Partnered Scheduled Bank)
Head Office : Troop Bazar , Hyderabad - 500 001 , Ph: +91-40 24685587

Notification

Request for Applications for Empanelment of Information System Auditors for Rural Cooperative Banks in the state of Telangana for 2020-21

1. Telangana State Cooperative Apex Bank Ltd, invites applications on the under-noted prescribed format from certified auditors who fulfills the eligibility criteria as mentioned here under and are willing to have their firms empaneled as Information System Auditor for conducting Information System Audit of Rural Cooperative Banks in the state of Telangana.
2. The profile should be submitted in the prescribed format enclosed herewith only to the Chief Information officer-ITSD, Telangana State Cooperative Apex Bank Limited, Head Office, TSCAB Buildings 3rd floor, Troop Bazar, Hyderabad-500001 only by e-mail.
3. " Application for Empanelment of Information System Auditors"
4. Applying professionals should submit soft copy of valid CISA certificate along with application, the copy of the certificate of CISA issued by ISACA certifying the candidate.
5. Incomplete application or applications without requisite enclosures will not be entertained.
6. Mere submission of application does not, in any way, constitute guarantee for empanelment /allotment of the audit job of any nature from the bank. The empanelment and allocation of the Banks to the auditors will be purely the prerogative of the Bank.
7. ***The eligibility criteria for such empanelment of candidate with the Bank are as under:***
    a. The right candidate shall have experience of information systems Audit of minimum three other Banks.
    b. Should be having CISA (ISACA) qualified.

The candidates fulfilling above criteria as applicable to them and narrated under para-1 to para-6 are requested to submit duly filled up application form and send the soft copy to cio_office@tscab.org along with copies of relevant certificates/ documents addressing to Chief Information officer-ITSD, latest by 15.02.2021

Note: Applicants can find the application form at 2nd page of this notification and can be downloaded from website under recruitments tab.

Terms and Conditions for Empanelment

1. AUDIT ASSIGNMENTS
    a. An Auditor will be contracted by TSCAB directly to perform information security audits.
    b. TSCAB may choose to associate its experts in audit assignments of an auditor to gain first-hand knowledge of quality of audits being carried out by the auditor.

2. RESPONSIBILITIES OF THE AUDITOR

    I. The Auditor shall ensure that:
        a. the scope of auditing assignment is defined clearly by the auditee
        b. the auditing is carried out strictly in accordance with the terms and conditions stipulated in the audit assignment contract as well as general expectations of the auditee from an auditor will be communicated in the detailed scope once we finalise the auditor empanelment.
        c. all applicable codes of conduct and auditing standards are adhered to with due professional care.
        d. the contract between the Auditor and the Auditee expressly permits access to the system for the Auditor and representatives of TSCAB, if need be, during audit assignments.
        e. the responsibility of the client data, that is preserved by the auditing organization, remains with the auditing organization.
        f. after sign off of the engagement, if the client's data is retained by the auditing organisation, then it must be encrypted and the access must only be provided on "Need to Know" basis.
        g. the auditing organization should not share the client's data without explicit written permission from auditee.
        h. the audit outcome & related matters should only be communicated to the specified Point of Contact (POC) of the auditee organization. The audit report should only be shared using secure methods such as use of passwords, encryption etc.
        i. Non-Disclosure Agreement (NDA) must be signed with the auditee organization before commencement of the project & must be legally enforceable. TSCAB Model NDA may be customized as per project/organization requirement.

    II. Information Security Auditing Organisations are mandatorily required to fill application form (i) Details of each & every audit conducted along with auditee details (ii) The critical vulnerabilities which were pointed during audit undertaken by them but not fixed by auditee organization even during follow up audits by auditing organization.

3. CONFIDENTIALITY
    The Auditor shall ensure that his employees, servants, agents and sub- contractors keep confidential all information in whatever form which is obtained, produced or derived from or related to the carrying out of its obligations under this terms and conditions as well as his Contract with the Bank(s).

4. QUALITY OFAUDIT

a. To ensure that the audit assignments are carried out in accordance with applicable guidelines and standards, TSCAB may review the audit work carried out by the empanelled Auditor and the qualifications of persons involved in Audit assignments. In addition, customer surveys may be used to assess the performance of an Auditor. Empanelled information security auditors should note that their continued empanelment status depends on the quality of auditing services rendered by them and the extent of user satisfaction, as may be reflected by them in their feedback. For the purpose of monitoring the quality of service, TSCAB may choose to-

- Carryout sample analysis of the information Security Audit work
- Depute its expert representatives to witness an Information Security Audit when the audit process is underway.
- Seek the opinion of the user auditee organisations.
- Analysis of Incident by TSCAB Team.
- Adopt any other means as deemed necessary.

b. Depending on the nature of outcome of above such suitable action, TSCAB may choose to either-

- Afford an opportunity to the auditor to effect necessary corrective action and demonstrate through suitable evidences or
- Temporarily withdraw or put on hold the empanelment status, as the case maybe.

5. TERMINATION OFEMPANELMENT OR DE-EMPANELMENT

a. Without prejudice to its rights under the Conditions of empanelment, TSCAB shall have the right to terminate empanelment of the Auditor at any time, if:

i. The Auditor breaches any of the terms and conditions;

ii. Degradation of auditor's performance or competence as per TSCAB assessment (Incident analysis, adverse reports, special skill test & related assessments)

iii. The Auditor’s performance or competence fails to meet the expectations required by the Audit assignment as per TSCAB view;

iv. In case, there is any change, which might affect the qualifying status of the Auditor and make them non-compliant with criteria as listed in “Guidelines for Empanelment by TSCAB”. (Auditing organizations are mandatorily required to bring to notice of TSCAB, if there is any change in their organization’s foreign tie ups or manpower or any other such changes relevant to empanelment by TSCAB. In case, such changes are not brought to immediate notice of TSCAB, it may lead to blacklisting of organization along with de-empanelment whenever it comes to knowledge of TSCAB)

v. Any lapses observed/reported in audits or in case, any of audit reports have not been submitted by auditing organisation to TSCAB.

b. Before exercising its options under the clause “a” in Point 6, where TSCAB considers the breach is capable of remedy, TSCAB shall notify the Auditor and afford an opportunity to remedy the breach within a reasonable time to be decided at the time

of notification to the Auditor. Provided the Auditor has rectified such a breach within stipulated period TSCAB shall not terminate the empanelment. If such a breach is not rectified within the stipulated period contained in the notification, then TSCAB has the right to terminate the empanelment with immediate effect. The decision of TSCAB shall be final and binding on the Auditor.

c. The Auditor shall, upon termination (for whatever reason), comply with all requests from TSCAB to return all documents and materials provided under or in relation to the Auditor empanelment and refrain from advertisement or making claims regarding the status of empanelment that can be viewed or interpreted as valid empanelment.

POINT OF CONTACT

Office of Chief Information Officer
Telangana State Cooperative Apex Bank Limited
Troop Bazar, Abids
Hyderabad - 500089

Expectations of TSCAB from an Auditor

1. Verifying possible vulnerable services only with explicit written permission from the auditee.
2. Refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
3. With or without a Non-Disclosure Agreement contract, the security auditor is ethically bound to confidentiality, non-disclosure of customer information, and security testing results.
4. The security auditor always assumes a limited amount of liability as per responsibility. Acceptable limited liability could be equal to the cost of service. This includes both malicious and non-malicious errors and project mismanagement.
5. Clarity in explaining the limits and dangers of the security test.
6. In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses is made known.
7. Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
8. The scope is clearly defined contractually before verifying vulnerable services.
9. The scope clearly explains the limits of the security test.
10. The test plan includes both calendar time and man-hours.
11. The test plan includes hours of testing.
12. The security auditors know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the customer organization.
13. The exploitation of Denial of Service tests is done only with explicit permission.
14. Social engineering and process testing are performed in non-identifying statistical means against untrained or non-security personnel.
15. Social engineering and process testing are performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
16. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing are reported immediately to the customer with a practical solution as soon as they are found.
17. Refrain from carrying out Distributed Denial of Service testing over the Internet.
18. Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
19. Notify the auditee whenever the auditor changes the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the customer is notified with progress updates at reasonable intervals.
20. Reports include all unknowns clearly marked as unknowns.
21. Reports state clearly all states of security found and not only failed security measures.
22. Reports use only qualitative metrics for gauging risks based on industry- accepted methods. These metrics are based on a mathematical formula and not on feelings of the auditor.
23. Auditee is notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
24. All communication channels for delivery of report are end to end confidential.

Audit Report content format

The formal information security audit report is a key audit output and must broadly contain the following:

- Identification of auditee (Address & contact information)
- Dates and Location(s) of audit
- Terms of reference (as agreed between the auditee and auditor), including the standard for audit, if any
- Audit plan
- Explicit reference to key auditee organisation documents (by date or version) including policy and procedure documents
- Additional mandatory or voluntary standards or regulations applicable to the auditee
- Summary of audit findings including identification tests, tools used and results of tests performed
- Analysis of vulnerabilities and issues of concern
- Recommendations for action & follow up audits
- Personnel involved in the audit, including identification of any trainees

Relevant details should be filled up with respect to the position as on date

Sl. No.	Particulars	Information required to be furnished by Candidates
1	**Name & address of the candidate**	enclose self-attested copy of relevant document with application form)
2	**Location of the candidate**	(enclose self-attested copy of relevant document with application form)
3	**Qualification and certifications**	**Name** **Certification** 1. 2. 3. 4. (enclose self-attested copy of relevant certificate of passing CISA with the application form)
4	**Experience of Bank IS Audit (should be supported by Appointment letter issued by individual banks)**	**Nature of audit** **Name of Bank** **Period** IS Audit : 1. 2. 3.
5	**Other experience including areas of specialization in Bank IS audits**	(enclose self-attested copy of relevant document with application form)
6	**Contact Nos. and e-mail address of the Candidates**	**Tel. No.** …….. **Mob. No.** …… **E-mail id**……
7	**Details of Blacklisting/ punishment by banks/ other institutions**	**Name of Bank/Institutions** **Nature of offence**
8	**Last IS Audit assignment, if any, undertaken for any bank**	**Nature of Assignment** **Period** **IS Audit**

I/We hereby declare that all the information submitted by me/us for empanelment is true and the certificates/documents attached are genuine. In case any information/documents is found as untrue/misleading, the Bank may take necessary action, including de-empanelment /blacklisting of the firms/members, as it may deem fit.

Signature of

candidate

Date:

Place:

NOTE: Bank reserves the right to ask for original copy of enclosed certificates for verification.