Empanelment Request Processing Fee : Rs. 5000/-Only (including Practical Skills Tests)

No. 3(15)/2004-CERT-In

Government of India

Ministry of Electronics and Information Technology

Indian Computer Emergency Response Team

(CERT-In)

Electronics Niketan, CGO Complex, Lodhi Road, New Delhi – 110 003

Guidelines for applying to CERT-In for Empanelment of IT Security AuditingOrganisations

Note:

1. Guidelines may be retained by the applicantorganisation.
2. Application Form, Annexure 'I', Annexure 'II', Annexure 'III' & Annexure 'A' should be filled in by the applicant IT Security auditing organisation & submitted to CERT-In along with the applicable requisitedocuments.

Indian Computer Emergency Response Team (CERT-In) empanel IT Security Auditing Organisations for auditing, including vulnerability assessment and penetration testing of computer systems, networks and applications of various organisations of the Government and those in other sectors of the Indian economy. The IT Security Auditing Organisations, so empanelled by CERT-In, will determine the effectiveness of IT Security controls over information resources and assets that support operations in the auditee organisations, and will determine vulnerabilities in their IT infrastructure. An IT Security Audit shall invariably comprise process, technology and people.

1. IT Security Audit and Assurance-Requirements

IT Security Auditing Organisations will be required to carry out the following:

a. Review of auditee's existing IT Security Policy and controls for their adequacy as per the best practices vis--à-vis established IT Security frameworks outlined in standards such as COBIT, cyber security framework, ITIL, ISO27001etc.
b. 'IT Security Audit' may involve a combination of thefollowing:
   i. NetworkMapping
   ii. Vulnerabilityassessment

iii. Exploitation of thevulnerabilities
iv. PenetrationTesting
v. Review and assessment of security policies and controls as per bestpractices
vi. Application securityassessment
vii. Log review, incidence response and forensicauditing
viii. Malware/Backdoordetection

c. Detailed 'Risk Assessment' and mapping of all 'Vulnerabilities' of systems and networks shall be documented, along with the security measures that are in place and the level of protection that theyprovide.
d. Detailed 'Penetration Tests' and possible exploitation of the 'Vulnerabilities' in the systems and networks shall be documented, along with the security measures that are in place and the level of protection that theyprovide.
e. Detailed 'IT Security Audit Report' clearly bringing out the actionable items shall need to beprepared.
f. The Auditor shall define 'IT Security Audit Methodology' being followed for conducting the IT Security Audit and ensure compliance with thesame.

2. Criteria forEmpanelment

2.1 TechnicalQualifications:

An applicant organisation, desirous of being empanelled as an IT Security Auditor, may be an organisation / company / firm providing IT Security auditing services. An applicant organisation must have the following minimum qualifications and experience:

a. Adequate knowledge and understanding of trusted computer information systems, telecommunication and networkingenvironment.
b. Should have minimum 5 no. of technical manpower with skills to perform technical security testing, especially vulnerability assessment & penetration tests, and should have the ability to analyse and evaluate theresults.
c. Should have personnel with information security related qualificationslike:
    i. Certified Information Systems Security Professional (CISSP),or
    ii. Certified Information Security Manager (CISM) of ISACA,or
    iii. Certified Information Systems Auditor (CISA) of ISACA,or
    iv. Diploma in Information Systems Audit (ISA or DISA) of ICAIor
    v. Any other formal IT Security relatedqualification
d. Preferably three years of experience in IT Security Auditing work as per the broad scope outlined in Para 1above.
e. Should have carried out at least five IT Security Audits, preferably two of which should be in the last 12 months in line with the broad scope outlined in Para 1 above

Note 1: Process audit experience in 'Scalable Monitoring Platform for the Internet (SCAMPI)' and /or 'Capability Maturity Model Based Assessment (CBA) Internal Process Improvement (IPI)' is desirable.

Note 2: In case of exceptional qualifications / experience, CERT-In reserves the right to waive off the conditions of professional's experience / qualification for individuals.

Note 3: IT Security compliance is a mandatory requirement for the critical sector organisations. Due to a Government directive or prevailing legal / regulatory provisions, only CERT-In empanelled IT Security auditing organisations are eligible to carry out such IT Security audits.

2.2 Commercial Contract:

Following empanelment, IT Security Auditing organisations will undertake to render the IT Security Auditing services in accordance with the terms & conditions of a commercial contract, to be solely executed between the auditee organisation and the empanelled IT Security Auditing organisations. It may be noted here that CERT-In is not a party to any such contract. Further, CERT-In would refrain from providing any sort of assistance to the empanelled IT Security Auditing Organisations in securing such acontract.

Forthepurposesofman-daycomputation,thefollowingdefinitionapplies:

"Auditing Man-day" shall mean IT Security auditing effort (both on-site as well as off- site) of minimum 8 hours, excluding breaks, by a person with suitable IT Security auditing related qualification such as CISSP, ISMS Lead Assessor, CISM, CISA, ISA or any other formal security auditing related qualification.

2.3 Quality ofAudits:

Empanelled IT Security auditing organisations may please note that their continued empanelment status depends on the quality of IT Security auditing service rendered by them and extent of user satisfaction as may be reflected in their feedback to CERT-In. All the empanelled IT Security auditing organisations are required to send bi-monthly report to CERT-In for the list of IT Security auditing work in hand / completed with duration (from date – to date) for overall assessment and review of the status of IT Security compliance inthecountry.Forthepurposeofmonitoringthequalityofservice,CERT-Inmaychooseto

-

- Carryout sample analysis of the IT Security auditingwork
- Depute its expert representatives to witness an IT Security audit when theaudit process isunderway.
- Seek the opinion of the user auditeeorganisations.
- Adopt any other means as deemednecessary.

Depending on the nature of outcome of above such suitable action, CERT-In may choose to either –

- Afford an opportunity to the IT Security auditing organisation to effect necessary corrective action and demonstrate through suitable evidencesor
- Temporarily withdraw or put on hold the empanelment status, as the case maybe

3. Submission of Response toCERT-In

The organisations, already providing auditing services in the area of IT Security, as well as desirous of being empanelled by CERT-In as an IT Security auditing organisation, should submit the requisite information in the prescribed format, as given in the document "Application Form for empanelment of IT Security Auditing Organisations by CERT-In". The applicant organisation will submit its application to CERT-In in an envelope, duly superscribed "Request for empanelment of IT Security Auditing Organisations" to the address givenbelow:

Empanelment Group,
Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Electronics Niketan, 6 C.G.O Complex,
Lodhi Road, New Delhi -110003

4. Procedure and Conditions for Empanelment

1. A duly constituted Technical Evaluation Committee (TEC) will evaluate the applicant organisations based on the essential criteria in documentation round. If necessary, applicants may be called for presentation to theTEC.
2. CERT-In shall test the vulnerability assessment and penetration testing capability of organisations through the practical skillstests.
3. CERT-In will publish the panel of successfull IT Security auditing organisation on its website.
4. The format of the IT Security audit report and the conditions of empanelment will also be communicated to auditee organisation. An auditee organisation will be free to choose any of the IT Security auditing organisations on the panel. CERT-In will have no role in that context.

5. It may be noted that CERT-In will not award any IT Security auditing assignment to any of the IT Security Auditors. An Auditee will have a direct relationship with an IT Security Auditing organisation selected by him from the Panel of IT Security Auditing organisations. However, CERT- In will monitor the quality of IT Security audit to ensure that it is in compliance with international best practices. From time to time CERT-In may choose to send its expert to an Auditee site when an IT Security audit isunderway.

6. Empanelment of the new organisations is a four step process followed by background verification & clearance by suitable Government agency, as givenbelow:

Step-1: Submission of Application Form (in the prescribed format) for empanelment of the organisation for 3 yearsw.r.t the year of empanelment, subject to complying with terms & conditions of empanelment,along with the following Annexures:

AnnexureI: Background verification certificate from the organization
Annexure II: ConsentForm
Annexure III: Undertaking by the organization on code of conduct
AnnexureA: Detailed information regarding last 5 information security audits carried out by organization during the last 3 years and copy of any two IT Security Audit Reports out of thesefive.

On assessment & verification of the documents submitted, the organization will be declared as successful or unsuccessful in step 1. Only organizations that are successful in Step 1 will be considered for step 2

Step-2: The organizations will be given two virtual images in DVD having some applications installed with the known vulnerabilities and possible penetrations built for the off-line in-house practical skills test, which they can test at their premises and should report at least 90% of known set of vulnerabilities and successful penetrations. Organization scoring 90% or more, on the basis of assessment of report, will be considered for Step 3. The organization will be given maximum two attempts to appear in offline PST.

Step 3: On being successful in Step 2, the qualified organizations will have to take an on-line practical skills test i.e. VA/PT PST and target a test-bed of known vulnerabilities and possible penetrations. Challenges will be declared in real time over IRC channel to the participating organizations. Organizations will be required to submit VA & PT report to CERT-In. Organization scoring 90% or more , on the basis of assessment of report, will be considered for step-4 i.e. Personal Interaction Session . The organization will be given maximum two attempts to appear in VA/PT PST.

Step-4: For the purpose of Personal Interaction Session, the TEC will meet in Delhi as well as in Bangalore to interact with the organizations who have qualified in step 3. This may include]

- Face to face meeting / Interaction with auditor team of suitable size. The team must have persons from the technical personnel informed to CERT-In as per the information form submitted toCERT-In.
- Interpretation of vulnerabilities and means of exploit by the auditororganization
- TechnicalCompetenceverificationatCERT-InorIIScBangalore,asdeemednecessary

7. Theassessmentofthereportedvulnerabilitiesandsuccessfulpenetrationswillbedoneagainstthemaster list of vulnerabilities and penetrations, prepared by CERT-In. Auditors are free to report any number of vulnerabilities, but their qualification depends on the number of vulnerabilities matching those in CERT-In's master list. So, it is in the interest of the organisations to report all the vulnerabilities and accomplishment of given challenges. In the assessment, all reported vulnerabilities, whether low, medium or high; and successful penetrations, will be given equal weightage.

8. An organization, clearing all the required steps of empanelment, will be eligible forempanelment subject to background verification and clearance of the organization and its technical persons by suitable Government Agency. The organization which is not given clearance after background verification by suitable Government Agency will not be empanelled by CERT-In even iforiganisation has cleared all the 4 steps as mentioned in clause no. 6

9. Special round of practical skill test is envisaged for the empanelled auditors in case some Complaint or reverse feedback on their technical competence and audit performance has been received from auditee organization or any other circumstances where creditability of empanelled auditors is suspected from technical point ofview.

10. As per the timelines published on CERT-In website, period of 3 months (From July to September every year) will be allocated for inviting the new applications in a year. Once empanelled, organisation will be empanelled for 3 years w.r.t year of empanelment, subject to complying with terms & conditions of empanelment.
    For example, if two organizations applied for empanelment from CERT-In in July-September 2020 and one of them gets empanelled on 1st July 2021, and the other one gets empanelled on 1st August 2021 then the validity of empanelment is till 30th June 2024 for both the organizations.

11. CERT-In reserves its right to ask the organisations for online access to test bed either throughthe static public IP at their premises, as submitted by the organisation, or from some other locations like CERT-In, IISc and few other places, as selected by CERT-In. These places will be under direct supervision / control of either officials from CERT-In or nominated byCERT-In.

12. After 2 (two) unsuccessful attempts in either offline in-house practical test or online VA/PT PST the organisation may apply as a fresh candidate after cooling off period of oneyear.

13. Forallfutureempanelments,Rs.5000/-willbechargedatthetimeofapplicationandrenewal thereafter.

14. CERT-In reserves the right to relax any qualifications for empanelment under exceptional circumstances.

15. Organisations registeredas Startup/ Micro, Small and Medium enterprises (MSME) can apply for CERT-In empanelment and request for relaxation in experience only.

16. CERT-In reserves its right to empanel the IT Security auditing organisations subject totheir compliance to empanelment qualification criteria & guidelines and acceptance of terms and conditions ofempanelment.

17. CERT-In reserves its right to accept any application in part or full or reject any or allthe applications without assigning anyreason.

18. CERT-In will not be a party to any commercial contract between an auditee organisation and anIT Security AuditingOrganisation.

19. CERT-Inwilllimititselftopublishingrelevantempanelmentinformationandwillnotofferanykind of assistance in securing a commercialcontract.

20. Empanelled IT Security Auditing Organisations shall undertake to keep confidential all the information that they have access to during the course of theiractions.

21. Empanelled IT Security Auditing Organisations shall ensure adherence to applicable codes of conduct and auditing standards with due professionalcare.

22. If any organisation, due to NDA between the auditing & auditee organisation, feels that it will be difficult for them to submit the copy of the two IT Security audit reports, then, if requested, CERT- In is ready to provide an undertaking for non-disclosure of the acquired information. So, such arguments for not submitting the IT Security audit reports will not beaccepted

23. Sample IT Security audit reports are notacceptable.

24. Sanitisation/MaskingoffinancialinformationonlyfromtheITSecurityauditreportsisacceptable.