Empanelment of Information Security

Auditing Organisations

-Terms and Conditions for Empanelment

by CERT-In

Version 7.1

Terms and Conditions for Empanelment

1. DURATION OF EMPANELMENT

1.1 The empanelment of an auditing organization is valid for 3 years from the 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.

1.2 Technical Evaluation Committee (TEC) will meet every year to discuss issues & processes related to the empanelment.

2 AUDIT ASSIGNMENTS

2.1 An Auditor will be contracted by a customer directly to perform information security audits. CERT-In is not a party to such contracts.

2.2 CERT-In 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.

3. RESPONSIBILITIES OF THE AUDITOR

3.1 The Auditor shall ensure that:

3.1.1 the scope of auditing assignment is defined clearly by the auditee

3.1.2 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 as outlined in Annexure I

3.1.3 all applicable codes of conduct and auditing standards are adhered to with due professional care

3.1.4 the contract between the Auditor and the Auditee expressly permits access to the system for the Auditor and representatives of CERT-In, if need be, during

Audit assignments.

3.1.5 the responsibility of the client data, that is preserved by the auditing organization , remains with the auditing organization.

3.1.6 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.

3.1.7 the auditing organization should not share the client's data without explicit written permission from auditee.

3.1.8 the auditing organization must have Incident Management Policy in place for handling incidents of data/confidentiality breach.

3.1.9 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

3.1.10 Non-Disclosure Agreement (NDA) must be signed with the auditee organization before commencement of the project & must be legally enforceable. CERT-In Model NDA may be customized as per project/organization requirement.

3.1.11 The auditing organisation should have signed NDA in place with all the employees.

3.2.1 Information Security Auditing Organisations are mandatorily required to fill in online 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.

3.2.2 In addition, it is mandatory for the auditor to share the consolidated report related to information Security audits quarterly with CERT-In as per format provided by CERT-In. It is also mandatory for the CERT-In empanelled auditing organization to report all the critical vulnerabilities along with auditee details to CERT-In on quarterly basis which were pointed by them during audit undertaken by them but not fixed by auditee organization even during follow up audits by auditing organization (as per format provided by CERT-In).

4. ADVERTISING

4.1 The Auditor shall not use the CERT-In logo, nor make any reference to the Auditor's association with CERT-In on any publicity material, promotional material or product without the prior written permission of CERT-In. Before CERT-In examines requests for permission, the Auditor shall submit the wording and presentation of such

information.

4.2 An Auditor may use the words “This Organisation is empanelled by CERT-In for providing information Security Auditing Service”. No other words shall be used to describe the Auditor’s relationship with CERT-In without the prior written permission of CERT-In. In such circumstances the proposed wording and presentation should be submitted as detailed in Clause 4.1 above.

4.3 The Auditor shall not use the CERT-In logo in any circumstances that would bring the Audit Service or CERT-In into disrepute.

5. LIABILITY IN RESPECT OF DAMAGE

5.1 The Auditor shall make good or compensate for, all damage occurring to Customer property in connection with a Contract with the Customer for carrying out an audit, provided that this Clause shall not apply to the extent that the Auditor is able to show that any Such damage was not caused or contributed to by the neglect or default of the Auditor or by any circumstances within his control.

6. INDEMNITY

6.1 The Auditor shall indemnify, and keep indemnified, CERT-In against all claims, demands, actions, costs, expenses, (including without limitation, damages for any loss of business, business interruption, loss of business information or other indirect loss), arising from or incurred by reason of any third party claims against CERT-In relating to or arising from the performance or nonperformance by the Auditor of any or all of its obligations under this terms and conditions as well as his Contract with the Customer.

6.2 Auditor shall indemnify auditee of the actual and liquidated damages which may be demanded by auditee.

7. CONFIDENTIALITY

7.1 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 Customer.

8. QUALITY OF AUDIT

8.1 To ensure that the audit assignments are carried out in accordance with applicable guidelines and standards, CERT-In 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, CERT-In 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 CERT-In Team.
- Adopt any other means as deemed necessary.

8.2 Depending on the nature of outcome of above such suitable action, CERT-In 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 may be.

9. TERMINATION OF EMPANELMENT OR DE-EMPANELMENT

9.1 Without prejudice to its rights under the Conditions of empanelment, CERT-In shall have the right to terminate empanelment of the Auditor at any time, if:

- The Auditor breaches any of the terms and conditions;
- Degradation of auditor's performance or competence as per CERT-In assessment (Incident analysis, adverse reports, special skill test & related assessments)
- The Auditor's performance or competence fails to meet the

expectations required by the Audit assignment as per CERT-In view;

- 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 CERT-In". (Auditing organizations are mandatorily required to bring to notice of CERT-In, if there is any change in their organization's foreign tie ups or manpower or any other such changes relevant to empanelment by CERT-In. In case, such changes are not brought to immediate notice of CERT-In, it may lead to blacklisting of organization along with de-empanelment whenever it comes to knowledge of CERT-In)
- Any lapses observed/reported in audits or in case, consecutive 3 quarterly audit reports have not been submitted by auditing organisation to CERT-In.
- Involvement in any sort of cyber security related assessment, unannounced access, penetration without prior written consent/approval of target entity.

9.2 Before exercising its options under the clause 9.1, where CERT-In considers the breach is capable of remedy, CERT-In 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 CERT-In shall not terminate the empanelment. If such a breach is not rectified within the stipulated period contained in the notification, then CERT-In has the right to terminate the empanelment with immediate effect. The decision of CERT-In shall be final and binding on the Auditor.

9.3 The Auditor shall, upon termination (for whatever reason), comply with all requests from CERT-In 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.

POINTS OF CONTACT

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

Phone: +91-11-24368572 / 24368551 Ext. 111

E-Mail: empanelment@cert-in.org.in

Expectations of an Auditee organisation from an Auditor **Annexure I**

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.

Annexure II

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