

Empanelment of IT Security Auditing Organisations

- *Terms and Conditions for Empanelment*

Version 2.0

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 non performance by the Auditor of any or all of its obligations under this terms and conditions as well as his Contract with the Customer.

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 IT 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 IT Security Audit work
- Depute its expert representatives to witness an IT Security Audit when the audit process is underway.
- Seek the opinion of the user auditee organisations.
- 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

- 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;
- In the view of CERT-In the Auditor's performance or competence fails to meet the standards required by the Audit assignment;
- There is a change, which might affect the qualifying status of the Auditor, (of which the Auditor shall give CERT-In notice at the earliest opportunity).

- 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

Dr. Gulshan Rai
Director, CERT-In,
Department of Information Technology,
CGO Complex, Lodhi Road, New Delhi – 110003
Tel: 011- 24368544
Fax: 011-24366806
eMail : saf@cert-in.org.in

Mr. B J Srinath
Scientist 'F', CERT-In,
Department of Information Technology
CGO Complex, Lodhi Road, New Delhi – 110003
Tel: 011- 24363138
Fax: 011-24368546
eMail : bsrinath@mit.gov.in

Mr. Omveer Singh,
Scientist 'D', CERT-In
Department of Information Technology
CGO Complex, Lodhi Road, New Delhi – 110003
Tel: 011- 24366793
Fax: 011-24368546
eMail : omveer@cert-in.org.in

Expectations of 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.

Report content format**Annexure II****1.0 Audit Report**

The formal IT security audit report is a key audit output and must 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 (See 2.0 below for a listing of typical reviews and tests that are performed during security audit)
- Analysis of vulnerabilities and issues of concern
- Recommendations for action
- Personnel involved in the audit, including identification of any trainees

2.0 List of typical reviews and tests**1. Review of security policies and procedures**

1. Review of organization IT security policy and management system
2. Review of security procedures including
 - a. Incident response
 - b. Business continuity planning and disaster recovery
 - c. Configuration management etc

2. Information Security Testing

1. Posture Assessment
2. Information Integrity Review
3. Intelligence Survey
4. Internet Document Grinding
5. Human Resources Review
6. Competitive Intelligence Scouting
7. Privacy Controls Review
8. Information Controls Review

3. Process Security Testing

1. Posture Review
2. Request Testing
3. Reverse Request Testing
4. Guided Suggestion Testing
5. Trusted Persons Testing

4. Internet Technology Security Testing

1. Logistics and Controls
2. Posture Review
3. Intrusion Detection Review
4. Network Surveying
5. System Services Identification
6. Competitive Intelligence Scouting
7. Privacy Review
8. Document Grinding

9. Internet Application Testing
10. Exploit Research and Verification
11. Routing
12. Trusted Systems Testing
13. Access Control Testing
14. Password Cracking
15. Containment Measures Testing
16. Survivability Review
17. Denial of Service Testing
18. Security Policy Review
19. Alert and Log Review

5. Communications Security Testing

1. Posture Review
2. PBX Review
3. Voicemail Testing
4. FAX Testing
5. Modem Survey
6. Remote Access Control Testing
7. Voice over IP Testing
8. X.25 Packet Switched Networks Testing

6. Wireless Security Testing

1. Posture Review
2. Electromagnetic Radiation (EMR) Testing
3. 802.11 Wireless Networks Testing
4. Bluetooth Networks Testing
5. Wireless Input Device Testing
6. Wireless Handheld Testing
7. Cordless Communications Testing
8. Wireless Surveillance Device Testing
9. Wireless Transaction Device Testing
10. RFID Testing
11. Infrared Testing
12. Privacy Review

7. Physical Security Testing

1. Posture Review
2. Access Controls Testing
3. Perimeter Review
4. Monitoring Review
5. Alarm Response Review
6. Location Review
7. Environment Review