Indian Computer Emergency Response Team

Guidelines for CERT-In Empanelled Information Security Auditing Organizations
Version 3.0

People

- Are courteous, cooperative, and professional.

- Have undergone a background check before employment. In case of employees moving from one CERT-In empanelled organization to another, a NOC / Relieving Letter shall be required from the previous organization as part of background check.

- For Government and critical sector audits, Organization must deploy manpower declared to CERT-In in snapshot information form. CERT-In reserves the right to verify/audit such information independently or from the auditing organization or the auditee organization.

- Have adequate competency in
    - security technology
    - security processes
    - security controls
    - security trends
    - fact collection
    - reporting

- Have high ethics and morals.

- Have experience and maturity in interacting with senior management and creating trust.

- Understand the consequences of their actions.

- Understand and ensure there is no conflict of interest.

- During and after the audit assignment are aware of information classification and know how to maintain confidentiality, security and privacy (such as collection, use, release, disclosure) of information and audit including but not limited to protecting against theft and damage of such information.

- Have signed Non-disclosure agreement(NDA) with the organization at the time of joining

- May need to sign NDA with the auditee organization depending upon the requirement of project under information to its employer organization.

Technical

- Auditors should help auditee organization in identifying the scope of work.

- Auditors must utilize industry standard methodologies, best practices for security testing. Solely tools based testing should be discouraged.

- Auditors should deploy a verification team (Red Team) to verify the work performed by their audit team (White Team).

- Auditor should clearly mention the environment in which the web application/ application has been tested in case of web application/ application security audit.

- Auditor will be required to audit and test the website on the staging server/testing environment provided by hosting service provider before issuing the audit certificate.

- Structure and Contents of final deliverable of the audit/testing (like vulnerability assessment report) should be finalized with the auditee organization before commencement of project.

- Refrain from carrying out Distributed Denial of Service testing over the Internet.

- Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.

- Refrain from testing and exploiting high risk vulnerabilities such as discovered breaches or which may put immediate lives at risk.

- Ensure appropriate approvals have been received in writing prior to carrying out any penetration tests and installation of tools and install tools in the presence of auditee system administrator.

- Ensure removal of tools after the completion of task and do not install any other software or damage any existing auditee software. Get acceptance of auditee for removal of tools in the presence of auditee system administrator.

- Ensure you provide a list of tools planned to be installed to auditee and provide a written confirmation to the auditee that you are not violating any IPR or license norms while using and installing the tools.

- Auditee related data should only be retained for specific period of time as in agreement with the auditee and disposed-off as per defined & agreed process. The collection, preservation and disposal of data collected by the auditor should be in accordance with the agreement entered between Auditor & Auditee. Auditor will ensure there is no mirroring of data outside the country. In any case, the auditor will not leak data at any time (during or after the audit) to any third party without the permission of Auditee. After wiping the data, auditing organization should also make sure that data cannot be retrieved by any known forensic technique.

Process

- Ensure a Formal Non-disclosure agreement is signed with the auditee and is in place prior to start of work.

- With or without a Non-Disclosure Agreement contract, the security auditor is ethically bound to confidentiality, non-disclosure of auditee information, and security testing results.

- Ensure that the timelines and commitments made to the auditee are adhered to.

- Ensure that there is no “expectation gap” in conducting an audit. The “expectation gap” is the difference between what perceive an audit to be and what the audit profession claim. Reduce or eliminate this by explaining in detail upfront the audit process, collection of artifacts and deliverables.

- All the observations made during the audit are well supported with objective evidences and all evidences are compiled carefully and correctly with the report.

- All the evidences gathered during the process of audit are presented in a manner that the decision makers are able to use them effectively in making credible risk based decisions.

- Audit report should mention appropriate timelines for closure of vulnerabilities according to severity.

- The security and confidentiality of the auditee data should be managed effectively and well established procedures should be defined and documented to handle auditee data during and after the audit.

- The information regarding audit team selected for conducting audit should be shared with the auditee and a documented approval regarding the same should be procured before the formal commencement of audit.

- CERT-In reserve the right to seek/audit information from auditing organizations for any project done within the time frame of empanelment period.

- Ensure that suggested controls and remedies are practical and implementable.

- Request auditee to provide feedback on the audit conducted to CERT-In as well as to you on completion of the audit.

- Ensure that CERT-In is not made a part of any contract between auditee and auditor.

- Be aware that CERT-In can be a part of the audit team to assess the quality and maturity of audit, if it so desires and the same should be communicated to the auditee.

- Auditor shall not use the CERT-In logo, nor make any reference to the Auditors 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.

- An Auditor may use the words “This Organization is empanelled by CERT-In for providing information Security Auditing Service”. No other words shall be used to describe the Auditors relationship with CERT-In without the prior written permission of CERT-In.

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

- 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 auditee.

- Provide quarterly report to CERT-In regarding generic information related to information security audits, number of audits carried out, the sector in which the audit has been carried out, the high level findings, new areas emerging for audit.

- It is responsibility of empanelled organization to keep CERT-In updated with snapshot information.

- Ensure to maintain a regular contact with the auditee after the audit has been completed and assignment is over, as a good business relationship. Auditors should setup a communication channel to inform/alert auditee about information security related latest development feasible to auditee environment.

- Auditee related data should be stored only on systems located in India with adequate safeguards and should keep the auditee informed of the means & location of storage and seek auditee’s consent where necessary. During project engagement, audit related data should be kept in encrypted form in auditor's laptop. Auditing organization should also ensure that data is wiped from auditor’s laptop after completion of the project.

- The sharing and disclosure of auditee related data, where necessary, should only be done with prior consent of auditee organization.The auditee/project related data should not be shared with or disclosed to any overseas partner, unless specifically authorized by the auditee.

- The audit outcome & related matters should only be communicated to the specified Point of Contact (POC) of the auditee organization. The audit outcome should only be shared using secure methods such as use of passwords, encryption etc.

- Auditing organization should prefer only official email id for sharing of audit report/data with auditee.

- Organization should have Incident Management Policy and related processes in place with clearly defined escalation matrix and procedures to deal with non-compliance. This process for dealing with incidents should be shared with the auditee.

- In case of the incidents where client audit related data is leaked to unauthorized entity (intentionally or unintentionally) , the auditing organization should inform the auditee of incident and take all necessary actions to address the incident as may be required.