
**Indian Computer Emergency Response Team**

# IT Security Auditing

## Guidelines for Auditee Organizations

Version 3.0

## A. INTRODUCTION

IT Security auditing is a critical component to test security robustness of information systems and networks for any organization and thus the selection of the most appropriate IT security auditor is a complex decision. IT security auditing is often considered for outsourcing owing to its highly specialized and technical nature. Considering the involvement of sensitive and confidential organizational data, it is vital that IT security auditor be capable and trustworthy.

IT Security auditing assignments can take many different forms depending upon the type and size of auditee organization. It is suggested that audit contracts be finalized only upon consultation with auditee's legal/contractual experts and after negotiations with the auditor. IT security auditing can be conducted as a separate activity or as part of the risk assessment process under the risk management program.

## B. AUDIT COMPONENTS AND CHARACTERISTICS

The auditor will need clear and unambiguous direction from auditee management (written rules of engagement), clearly defined scope for security audit and input on what is required for planning & assessment, requirement analysis, test execution & analysis, results and documentation.

### B.1 Introduction

Identifies the purpose, participants (auditee & auditor organization and any other),Technical team(both auditee and auditing organization), Briefing schedule and audit scope definition.

### B.2 Audit Environment

Describes the environment in which the auditor will perform the audit including the physical location, hardware/software being used, policy and procedures the auditor will need to follow. Key components are:

2.2.1 Entities and Locations
2.2.2 Facilities at each location
2.2.3 Equipment at each location
2.2.4 Policies, Procedures and Standards
2.2.5 Agreement and Licenses

**B.3** Roles and Responsibility

In case any of the activities to be audited in the auditee organization are outsourced, auditee must ensure that relevant personnel from outsourced organization are available at the time of audit. The auditor's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions and *modus operandi*.

**Please Note:**

*"Auditing Man day" shall mean auditing effort (both on-site as well as off-site) of minimum 8 hours, excluding breaks, by a person with suitable auditor qualification such as CISA/CISSP/BS 7799 Lead Assessor/ISA or any other formal security auditor qualification.*

**B.3.1** Auditor Organization Responsibilities: The contract should include clear identification of the following:

**B.3.1.1** Audit Checklist (Mutually agreed upon by the Parties)

**B.3.1.2** Audit Plan with timelines (Mutually agreed upon by the Parties)

**B.3.1.1** Audit tasks

**B.3.1.2** Documentation requirements

**B.3.1.3** Audit Support requirements

**B.3.1.4** Reporting Requirements: Structure, Content and secure handling of final deliverable (Such as Audit Reports) should be mutually agreed by the auditee and auditing organization.

**B.3.1.5** For critical and government sector organizations, Auditor must only deploy the manpower with background verification check done from suitable Law Enforcement Agency.

**B.3.2** Auditee Organization Responsibilities: Besides the conditions that get specified in the contract, the following form part of auditee obligations:

**B.3.2.1** Auditee refrains from carrying out any unusual or major network changes during auditing/testing.

**B.3.2.2** To prevent temporary raise in security only for the duration of the test, the auditee notifies only key people about the auditing/testing. It is the auditee's judgment, which discerns who the key people are; however, it is assumed that they will be people at policy making level, managers of security processes,

incident response, and security operations.

**B.3.2.3** If necessary for privileged testing, the auditee must only provide temporary access tokens , login credentials, certificates, secure ID numbers etc. and ensure that privilege is removed after the audit.

**B.3.2.4** A Technical team should be assigned as point of contact by the auditee organization for assisting and monitoring the auditors during the audit and the details of the technical team should be shared with the concerned auditors. Auditee should assure and schedule regular interaction of technical team with auditors.

**B.3.2.5** A Formal Confidentiality & Non-disclosure agreement must be signed with the auditor before starting of the work.

**B.3.2.6** There should be a well defined escalation matrix both for the auditee and auditing organization for addressing any problem encountered during the audit process which should be shared with respective authorities.

**B.3.2.7** A well defined mechanism must be in place which clearly states the procedure in which the report would be stored and destroyed after the completion of audit by the auditing organization. Thus, the mechanism should be designed in such a way that it confirms the following:

- Secure handling of report at transit.
- Secure handling of report at rest.
- Disposal time of report and related information by auditor.

**B.4** Terms and Adjustments

This section provides details about:

**B.4.1** Costs
**B.4.2** Periods of Performance with Deliverables and Timelines
**B.4.3** Dispute Resolution
**B.4.4** Remedies for Non-Compliance
**B.4.5** Maintenance of Agreements

## C.AUDITEE EXPECTATIONS

The following are the expectations of auditee organization from an auditor:

- **C.1** Verifying possible vulnerable services only with explicit written permission from the auditee.
- **C.2** Auditors must verify the existing policies of the organization against the industry standards and best practices and suggest the necessary improvements if required.
- **C.3** Refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
- **C.4** A formal Confidentiality & Non-disclosure agreement should be signed by the IT Security auditing organization prior to commencing the cyber security auditing work. The auditing organization and its auditors are ethically bound to maintain confidentiality, non-disclosure of auditee information, and security testing results.
- **C.5** 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).
- **C.6** Clarity in explaining the limits and dangers of the security test.
- **C.7** In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses is made known and a formal written permission with a clear definition of the tasks to be performed should be taken.
- **C.8** Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
- **C.9** The scope is clearly defined contractually before verifying vulnerable services.
- **C.10** The scope clearly explains the limits of the security test.
- **C.11** The test plan includes both calendar time and man-hours.
- **C.12** The test plan includes hours of testing.
- **C.13** 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 and the result of such testing should be approved formally by the authorized person of auditee organization.
- **C.14** The exploitation of Denial of Service tests is done only with explicit permission.
- **C.15** Social engineering and process testing are performed in non-identifying statistical means against untrained or non-security personnel.
- **C.16** Social engineering and process testing are performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
- **C.17** 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.
- **C.18** Refrain from carrying out Distributed Denial of Service testing over the Internet.

**C.19** Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.

**C.20** 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.

**C.21** Reports include all unknowns clearly marked as unknowns.

**C.22** All conclusion should be clearly stated in the report with the clear objective evidence for each conclusion drawn.

**C.23** Reports use only qualitative metrics for gauging risks based on industry-accepted methods.

**C.24** Auditee is notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.

**C.25** All communication channels for delivery of report are end to end confidential.

## D. GENERAL GUIDELINES

**D.1** Auditee must implement the guidelines and advisories issued by CERT-In and/or suitable Government Agency time to time in their auditing program.

**D.2** Regular interaction framework during audit should be setup.

**D.3** Auditee should interview manpower deployed by auditor for conducting the audit.

**D.4** Ensure that auditor is utilizing industry standard methodologies, best practices for security testing.

**D.5** Scope of audit (in case of VA/PT) should not be limited to the few lists like OWASP top 10 or SANS Top 25 programming errors, it must include discovery of all known vulnerabilities.

**D.6** Auditee must demand for the working notes upon completion of the audit (provisions for this must be made in the audit contract itself) and should ask for audit evidences collected to be submitted as appendix along with the final audit report.

**D.7** Audit report format should be mutually agreed upon (Auditee and Auditor) and finalized before commencement of the audit. A sample web-application audit report for reference is available at Annexure-I.

**D.8** Regular meetings should be held between the auditor and auditee representatives (SPOCs) to review the progress of the audit in order to assess and improve the audit efficiency.

**D.9** Auditee must ensure that the tests agreed upon in the audit contract are actually being conducted by the auditor and also that the prescribed timeline is being followed, through the aforementioned meetings.

**D.10** CERT-In empanelled auditors are selected after much scrutiny and testing but it is vital to understand that while the list of empanelled auditors is true and accurate, CERT-In cannot guarantee the authenticity of audit details provided by these organizations.

**D.11** While selecting an auditor, it is the responsibility of the auditee to check the domain audit conducted, previous audits conducted and other relevant details. An auditee should have a clear understanding of the auditor's audit methodology, tools use, experience in the relevant domain and all available alternatives like other competent organizations before selecting.

**D.12** If the credibility of the auditor is unclear, auditee must make sure that the contractual agreement allows the auditee to stop the audit and choose another auditor within a reasonable duration of time in order to avoid financial losses on both ends.

**D.13** Feedbacks/complaints to CERT-In help improve the quality of selecting auditing organizations in future, thus, it is both an auditee's right and duty to provide relevant feedbacks. All feedbacks/complaints are kept confidential and are acted upon promptly with utmost importance.

**D.14** Last but not least, the auditee must act upon the relevant audit findings and strive to improve the IT security.

## E. SNAPSHOT INFORMATION & TECHNICAL MANPOWER DETAILS

Information about the CERT-In empanelled Auditing organization is availableat CERT-In website.

The information provided on the CERT-In website can help the auditee organization with respect to the following:

- Evaluation of man power and skillset details of an auditing organization
- Experience of an auditing firm relevant to information security audits
- Categories of information security audit conducted by the auditing organization
- Information security audits carried out by an organization in last 12 months(sector wise)
- Category wise number of audits conducted by an organization in last 12 months
- Technical man power deployed for audits by an organization with details
- Tools used in various audits

**NOTE -**Snapshot information available at CERT-In website is as provided by the respective organizations. The Information is not verified by CERT-In and thus CERT-In does not hold any responsibility in case of any discrepancy found in the information.

## F. THIRD PARTY HOSTING SERVICE PROVIDER

In case a services/website is hosted on a webserver owned by another organization, then the webserver system,its operating system and webhosting application software including backend database application software, if any, are under the control of the organization hosting the website (i.e. owning the webserver) and it is the responsibility of webserver owner to take care of information security auditing of these, as the organization owning the website contents does not have any access or control over these assets.

However, since the data / software related to the web-site are under the control of the organization owning the contents of the website, their responsibility is limited to get these audited by a CERT-In empanelled information security auditing organization.

The organization, owning the website contents, can select any auditing organization out of the CERT-In empanelled information security auditing organizations as per their office rules & procedures and financial guidelines to get these audited. The information security audit report from the information security auditor should clearly state that these webpages, including the backend database and scripts, if any, are free from any vulnerability and malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website.

## E. RELATIONSHIP AUDITEE & AUDITOR

Auditing process is aimed for the continual improvement of the auditee organization and thus the auditor perspective should be aimed at refining the security process rather than merely complying with the standard against which the auditing is done. The Auditing organization must maintain a relationship with the auditee even after the completion of the audit process to keep auditee organization updated for the latest security developments and to help in implementing the secure environment.

## G. DISCLAIMER

The outline provided here must be treated only as a guide/standard format by the auditee; the specific formats and terms & conditions of auditors will be unique for each organization.

**Annexure-I**

# Sample Report Format for Web-application Security Audit

**Audit Conducted for (Name of Auditee Organisation):**

**Audit Conducted by (Contact Person details with email and mobile):**

**Report Submitted On (Date):**

**Test duration: From (Date) _____ To (Date) _____**

**URL/IP addresses of the Web-Application:**

**Report Reviewed by:**

**Report Handed over to (Name and contact details of person from auditee organization):**

# I. Executive summary:

**Section-I**

*<Overview of scope, audit methodologies, tools used, observations, etc. >*

**Section-II**

*List of vulnerable points*

*<Separate table for each IP tested>*

***IP Address with URL*** *<Description of machine (IP/OS/Services running)>*

| **S.no.** | **Vulnerable point/Location** | **Vulnerability** | **Mean of identification**<br>**Manually/Tool**<br>**(if tool mention the name)** | **Comments/review of flaw** |
|---|---|---|---|---|
| | | | | |

## II. Vulnerability Assessment:

**Section-I**

*<Separate section for each IP>*

**IP with URL :** <details of machine IP/OS/ services>

*<for each vulnerable point>*

**Vulnerable Point-1/2/3..../n**

a. Vulnerable Point:
b. Name of Vulnerability:
c. Steps of verification of vulnerability(Proof of concept) with screenshots:

**Section-II** *<if penetration testing is in scope>*

*<for each penetration>*

**Penetration-I/II/III/IV:**

Machine Detail: <IP/URL/OS/Service>

Vulnerabilities used for exploitation:

Proof of concept with screenshots: <Step by Step- detail description of Penetration>

## Details of Team engaged for audit:

| S.No. | Name | Email and phone | Qualification and certification |
|---|---|---|---|
| | | | |