

SHRI LAL BHADUR SHASTRI NATIONAL SANSKRIT UNIVERSITY

(A Central University)

B-4, Qutub Institutional Area, New Delhi-110016.

(Under Ministry of Education, Govt. of India)



Ref. No: F.11()/LBSU/CC/IT-Audit/205

Dated : 21.06.2023

To,

All CERT-IN empanelled IT Auditors

Sub:- Quotation for IT Audit of IT infrastructure of the University.

Dear Sir,

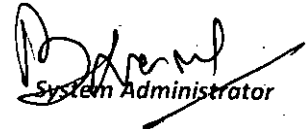
The sealed quotations are invited from the CERT-IN empanelled IT Auditors for the University IT Infrastructure Audit as per the following terms & conditions with the scope of work at Annexure I and under the certain IT Security auditing guidelines at Annexure II.

- The last date and time of Submission of quotations : 05/07/2023 up to 3.00 PM
- Date and time of opening of quotations : 05/07/2023 up to 3.30 PM

Terms & Conditions:

1. The service provider must be CERT-IN empanelled IT Auditor.
2. Bidder should be ISO9001 and 27001 certified
3. The service provider must have at least 30 CISSP/CISM/CISA/DISA/CEH certified professional as employees.
4. The service provider should not be blacklisted /barred by GOI, State government or any other regulatory of India.
5. The Service provider must have at least 03 years' experience in offering IT security Audit service in Govt./PSU organization under CERT-IN empanelment .

You are requested to submit your sealed quotation addressed to the Registrar, SLBS National Sanskrit University, B-4, Qutub Institutional Area, New Delhi-16 in the Computer Centre of the University. The envelope containing the quotation should be marked "Quotation for IT audit of IT Infrastructure of the University". The University reserves the right to cancel all the quotations without assigning any reason whatsoever.


System Administrator



SHRI LAL BAHADUR SHASTRI NATIONAL SANSKRIT UNIVERSITY

(A Central University)

B-4, QUTUB INSTITUTIONAL AREA, NEW DELHI-110016

(Under Ministry of Education, Govt. of India)

(IT -Audit of All IT INFRASTRUCTURES)

A. Project objective

Shri Lal Bahadur Shastri National Sanskrit University, Under Ministry of Education, Govt. of India is interested to undertake IT Infrastructure security audit, as per cert-in guidelines so as to establish a baseline assessment of security as it appears from outside the organization's network boundaries, internal network devices, servers and Network Storages. The penetration test involves gathering information about the University information systems and security infrastructure, and then using this information to attempt to identify and then exploit known or potential security vulnerabilities. Suggest mitigation strategies for the gaps identified.

Based on the contents of the University, the selected Bidder shall be required to independently arrive at approach and methodology, based on CERT-In guidelines. The approach and methodology will be approved by the University. The selected Bidder shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment.

B. Project Scope

Vulnerability Assessment and Penetration Testing should cover the all Servers, Desktops, Thin client, Networking systems, Security devices etc. Maintained at the University premises. Selected bidder should carry out an assessment of Threat & Vulnerabilities assessments and assess the risks in the University IT Infrastructure. This will include identifying existing threats if any and suggest remedial solutions and recommendations of the same to mitigate all identified risks, with the objective of enhancing the security of Information Systems. Bidder shall perform the onsite audit & assessment of the assets under the Scope of the University.

C. Penetration testing:

Penetration testing is to be carried out to ensure the security of Information systems and services, so that security weaknesses can be identified and then fixed before they get exposed. The frequency and severity of network intrusion, data theft and attacks caused by malicious code, hackers, disgruntled employees continues to increase and the risks and costs associated with network security breaches and data theft are astronomical. These may eventually give an intruder access to sensitive information. Using penetration testing tools can significantly reduce the risk of this occurring.

The principal objective of penetration testing is to determine security weaknesses in the University network infrastructure. The reasons to perform a network penetration test will be:

- a) To understand the current security posture by identifying gaps in security. This enables the University to develop an action plan to minimize the threat of attack or misuse.
- b) Helps in creating a strong reason to justify a needed increase in the security budget or make the security message heard at the Competent Authority level.
- c) A penetration test and an unbiased security analysis enable organizations to focus internal Security resources where they are needed.
- d) Penetration testing tools help organization meet these regulatory compliances.

D. Scope of work:

To carry out the Vulnerability assessment & penetration testing to determine security weaknesses in the University network infrastructure using procedures to be performed from outside and inside the organization's systems, that is, from the Internet or Extranet and LAN. The test typically begins with publicly accessible information about the client, followed by network enumeration, targeting the University's externally visible servers or network devices. A typical systems audit for the University would include the following:

- i) IT General Controls Audit
- ii) Network Security Audit
- iii) Vulnerability Assessment Penetration Testing
- iv) Physical and Environmental Security Audit for the review of Data Centers/ Server Rooms.

E. The types of devices for VAPT are as listed below:

Sr. No.	Device type	No of devices
1	Desktops & Thin Client	495 (Approx.)
2	Servers & Storages.	28 Virtual Machine
3	Network Devices	30 (Firewall, Core Switch etc.)
4	Public IP (For, Firewall & others)	16 Public IP
5	Access Point	37

F) Scope of work for Vulnerability Assessment

(i) General aspects for all systems

- ✓ Access control and authentication
- ✓ Network settings
- ✓ General system configuration
- ✓ Logging and auditing
- ✓ Password and account policies
- ✓ Patches and updates

(ii) Specific requirements for Server/OS Configuration Audit

- ✓ File system security
- ✓ Account Policies
- ✓ Access Control
- ✓ Network Settings
- ✓ System Authentication
- ✓ Logging and Auditing
- ✓ Patches and Updates
- ✓ Unnecessary services
- ✓ Remote login settings
- ✓ Vulnerability assessment of servers
- ✓ Secured Operating System Installation
- ✓ Patch and Service Pack levels for the Operating Systems as applicable
- ✓ Users and Groups created, including user management, password complexity, etc.
- ✓ File system security of the OS (to include file integrity checks in addition to access control)
- ✓ Access rights and privileges
- ✓ Services and ports accessible
- ✓ Change management in terms of modification to the Operating System
- ✓ Backup and emergency response measures
- ✓ Create baseline of critical parameters of the servers and OS configurations

- ✓ Determine anti-virus configurations, architecture, definition dates, scanning and updating policies.

(iii) Configuration Audit of Networking & Security Devices

- ✓ Access Control
- ✓ System Authentication
- ✓ Auditing and Logging
- ✓ Insecure Dynamic Routing Configuration
- ✓ Insecure Service Configuration
- ✓ Insecure TCP/IP Parameters
- ✓ System Insecurities
- ✓ Unnecessary services
- ✓ Remote login settings
- ✓ Latest software version and patches

(iv) Firewall/ VPN Audit

- ✓ Check for default configuration of the Firewall/ Switches
- ✓ Response to various protocols like TCP, UDP, ICMP, etc.
- ✓ List of open ports available for external users
- ✓ Verify Rule sets for Admin access, Lockdown rule, internal user, External user, Web server access, Pop access to mail server, Access to ICQ connections
- ✓ Audit of DMZ configuration
- ✓ VVPN Policies
- ✓ VPN configuration access
- ✓ VPN access controls
- ✓ Logging
- ✓ Log functions viz. File location, Integrity and confidentiality of logs, Log analysis, and Log rotation
- ✓ Change control - modification of rule base, up gradation of Checkpoint etc.
- ✓ Audit of Authentication mechanism (if used)
- ✓ Audit of Encryption method (if used)
- ✓ Third party software used with Firewall for additional services
- ✓ Firewall failure mode - fail open or fail secure
- ✓ Ease of recovery and backup of Firewall

(vii) Audit of Physical and Environmental Security

- ✓ To review the physical security measures in place to ensure physical security of information and information systems.
- ✓ To conduct a thorough examination of the physical environment in which all network devices and server reside
- ✓ To study the existing infrastructure from the security and accessibility point of view.
- ✓ To identify the general physical security concerns, and suggest provision for enhancing the physical security of the devices.

(viii) Desktop Security Audit

- ✓ Virus signatures and updates on desktop
- ✓ Adherence to System Usage Policies
- ✓ Shared folders access-control
- ✓ Services
- ✓ Windows and other patches
- ✓ Clear-desk and clear-screen policy
- ✓ Presence of unnecessary software

(ix) Security configuration:

Desktops/laptops/workstations that are used by the University users should be performed on sampling basis to ensure that Active Directory Services are effectively implemented in the Department along with the relevant security policies concerned.

(x) Vulnerability Assessment:

As part of the vulnerability assessment exercise, the security consultants are required to sit with the system administrators to assess the security configuration of the devices, identify misconfigurations and to provide the assurance on the security

controls placed on the given system. This is in addition to the execution of automated tools.

(xi) Scope of Work Penetration testing

- ✓ Man in the browser attack
- ✓ Any other attacks.
- ✓ Test for default passwords
- ✓ Test for DOS vulnerabilities
- ✓ Test for directory Traversal
- ✓ Test for insecure services such as SNMP
- ✓ Check for vulnerabilities based on version of device/server
- ✓ Check for weak encryption
- ✓ Check for SMTP related vulnerabilities such as open mail relay
- ✓ Check for strong authentication scheme
- ✓ Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
- ✓ Test for information disclosure such as internal IP disclosure
- ✓ Look for potential backdoors
- ✓ Check for older vulnerable version
- ✓ Remote code execution
- ✓ Weak SSL Certificate and Ciphers
- ✓ Missing patches and versions
- ✓ This is a minimum indicative list, CERT-IN auditors are encouraged to check for more settings in line with best practices including PCI, OSSIM etc.

(xii) VAPT for infrastructure should be comprehensive but not limited to following activities:

- ✓ Network Scanning
- ✓ Port Scanning
- ✓ System Identification & Trusted System Scanning
- ✓ Vulnerability Scanning
- ✓ Malware Scanning
- ✓ Spoofing
- ✓ Scenario Analysis
- ✓ OS Fingerprinting
- ✓ Service Fingerprinting
- ✓ Access Control Mapping
- ✓ Denial of Service (DOS) Attacks
- ✓ DDOS Attacks
- ✓ Authorization Testing
- ✓ Lockout Testing
- ✓ Password Cracking
- ✓ Cookie Security
- ✓ Functional validations
- ✓ Containment Measure Testing
- ✓ War Dialing
- ✓ DMZ Network Architecture Review
- ✓ Firewall Rule Base Review
- ✓ Server Assessment (OS Security Configuration)
- ✓ Security Device Assessment
- ✓ Network Device Assessment
- ✓ Database Assessment
- ✓ Vulnerability Research & Verification
- ✓ Man in the Middle attack
- ✓ All documents will be handed over in soft copy format.
- ✓ Soft copies of all the documents properly encrypted/ password protected in MS Word /MS Excel /PDF format

G) Security testing methodology should involve the following stages:

- a. Profiling the target network and identifying vulnerabilities
- b. Conduct tests to determine if the vulnerabilities can be exploited
- c. Conduct in-depth configuration reviews of critical systems, network devices and desktops to identify security gaps
- d. Suggest mitigation strategies for the gaps identified and submit first hand report

- e. Conduct test & in-depth configuration review after suggestion and patching the gaps at the first hand report (Mostly on public IPs).
- f. submit the final report of VAPT to the organization

H) The scope includes OWASP, OSSTM methodologies / phases for carrying out the network vulnerability analysis and penetration test from outside (Offline) through internet and Inside on the local LAN at single location in the University.

(I) Any other methodologies: required to carry out the vulnerability analysis penetration testing and involves use of effective guidelines, methods and tools to ensure that the exercise carried out is meaningful.

(J) The VAPT Report should contain the following: -

- ✓ Identification of Audited (Address & contact information)
- ✓ Dates and Locations of VAPT
- ✓ Terms of reference
- ✓ Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, website assessment, etc.)
- ✓ Tools used and methodology employed
- ✓ Positive security aspects identified List of vulnerabilities identified Description of vulnerability
- ✓ Risk rating or severity of vulnerability
- ✓ Category of Risk: Very High (Critical) /High/ Medium/ Low
- ✓ Test cases used for assessing the vulnerabilities
- ✓ Illustration of the test cases
- ✓ Corrective steps / methodology
- ✓ Analysis of vulnerabilities and issues of concern
- ✓ Recommendations for corrective action
- ✓ Personnel involved in the audit

The Bidder may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. All the gaps, deficiencies, vulnerabilities observed shall be thoroughly discussed with respective the University officials before finalization of the report.

(K) Compliance Audit

After the primary audit report, the University shall patch up all the vulnerabilities. Once the vulnerabilities are patched, compliance audit to be carried out by the bidder and final compliance certificate to be provided by the bidder. Time period of 2 to 4 weeks to be provided to comply with the audit recommendation.

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to with stand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks. The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques. The penetration tests should cover but not limited to OWASP Top 10 attacks.

(L) Bill of Quantity

Sr. No.	Component	Qty.	Unit	Unit Rate(Rs.)	Total Without GST(Rs.)	GST in %	Total inclusive of GST(Rs.)
1.	Stage-I VAPT Audit	1	NO				
2.	Stage-II VAPT Compliance Audit	1	NO				

Note:-

- The payment for stage I VAPT audit will be paid on submission of audit report for which Auditors should be available for at the University during Stage-I VAPT audit.
- The payment for stage II VAPT audit will be paid on
- submission of audit report for which Auditors should be available for or more at the University during Stage-II compliance VAPT audit.
- The rates are to be quoted accordingly.

(M) Eligibility and Evaluation of Auditor / Service provider.

Sr.No.	Clause	Required Documents
1.	The service provider must be empaneled from CERT-IN.	Proof of Cert-In empanelment Vendor
2.	Bidder should be ISO9001 and 27001 certified	Certificate
3.	Bidder Should have minimum average turnover of 01 cr. In last three FY.	Balance Sheet last 03 years
4.	The service provider must have at least 30 CISSP/CISM/CISA/DISA/CEH certified professional as employees.	List of employee with Name & work profile
5.	The service provider should not be blacklisted /barred by GOI, State government or any other regulatory of India..	Self-declaration Certificate with Authorized signatory
6.	The Service provider must have at-least 03 years experience in offering IT security Audit service in Govt./PSU organization under CERT-IN empanelment .	Similar work order with completion Certificate
7.	Enclosed others Documents	Certification of In-corporation, PAN, GST Certificates.

(I/We hereby agree to all the technical terms and conditions)

.....
Signature and seal of the Tenderer with date



Handling Computer Security Incidents

Indian Computer Emergency Response Team

IT Security Auditing

Guidelines for Auditee Organizations

Version 5.0

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 and data at transit.
- Secure handling of report and data 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** Auditing organizations must comply with all applicable regulations, acts/Circulars from Government & Regulators with respect to data security & privacy.
- C.6** 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.7** Clarity in explaining the limits and dangers of the security test.
- C.8** 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.9** Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
- C.10** The scope is clearly defined contractually before verifying vulnerable services.
- C.11** The scope clearly explains the limits of the security test.
- C.12** The test plan includes both calendar time and man-hours.
- C.13** The test plan includes hours of testing.
- C.14** 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.15** The exploitation of Denial of Service tests is done only with explicit permission.
- C.16** Social engineering and process testing are performed in non-identifying statistical means against untrained or non-security personnel.
- C.17** 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.18** 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.19** Refrain from carrying out Distributed Denial of Service testing over the Internet.
- C.20** Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
- C.21** 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.22** Reports include all unknowns clearly marked as unknowns.
- C.23** All conclusion should be clearly stated in the report with the clear objective evidence for each conclusion drawn.
- C.24** Reports use only qualitative metrics for gauging risks based on industry-accepted methods.
- C.25** Auditee is notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
- C.26** 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 organizations need to verify the technical credentials of the manpower deployed for the audit at their end in line with the qualification requirement mentioned at "Guidelines for applying for Empanelment" and auditee should interview manpower deployed by auditor for conducting the audit.
- D.4** Auditee will ensure from Auditor that audit related data should be stored only on systems located in India with adequate safeguards.
- D.5** Ensure that auditor is utilizing industry standard methodologies, best practices for security testing.
- D.6** 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.7** 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.

Indian Computer Emergency Response Team

- D.8** 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.9** 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.10** 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.11** 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.12** While selecting an auditor, it is the responsibility of the auditee to check the domain of audit conducted, previous audits conducted and other relevant details. An auditee should have a clear understanding of the auditor's audit methodology, tools used, experience in the relevant domain and all available alternatives like other competent organizations before selecting.
- D.13** 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.14** 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.15** Last but not least, the auditee must act upon the relevant audit findings and strive to improve the IT security.
- D.16** Auditee Organisation are required to verify credentials of CERT-In empanelled organisation, before availing their services, by checking their details in the list of CERT-In empanelled information security organisations.
Don't fall prey to fake organisation posing as CERT-In Empanelled Information Security Organisation.

E. SNAPSHOT INFORMATION & TECHNICAL MANPOWER DETAILS

Information about the CERT-In empanelled Auditing organization is available at 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 audit

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.Executivesummary:

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 Manually/Tool (if tool mention the name)

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>



Indian Computer Emergency Response Team

Details of Team engaged for audit:

S.No.	Name	Email and phone	Qualification and certification