Minimum Scope**of Cyber Security Audit and VAPT**

1. **Cyber Audit**
2. **Scope:** Cyber security audit should check the entity’s compliance to SEBI circulars, advisories and NCIIPC control guidelines. The Implementation audit, configuration audit and change management audit of the ICT should be focused as part of the audit scope and the same should be made part of audit report submission.
3. The functional efficacy of the SOC need to be checked to check the threat detection and response capabilities. The testing may be done through means of purple team/Penetration Testing exercises, cyber drills, analysis of action taken on threat alert reports as part of audit etc. The auditor shall examine these minimum parameters mandatorily: -
   1. Quality of logs being examined at SOC. Viz. logs from ***all*** security devices, applications, databases, OS, servers, cloud hosted servers, end points and network devices, their verbosity and their correlation at SOC.
   2. Efficacy of SOC rules and use case scenarios to detect and respond to all relevant signature based and behavior-based attacks. keeping the latest attack techniques also in mind.
   3. Detection, response and threat hunting capability of the SOC personnel.
4. Auditors shall also examine the consistency and efficacy of implemented security configurations of operating systems, databases, security devices, network devices, end points and servers etc. against the baseline standards.
5. Auditors shall examine in detail whether whitelisting approach has been implemented by the entity or not. Whitelisting in terms of blocking all the connections (inbound and outbound) with proper ACL implementation following the white list approach that allows ***only*** good known IP’s / ports / calls / applications / services / protocols etc. shall be examined Any discrepancy shall be categorically documented in the findings.
6. Auditor shall also carefully examine the readiness of the organization and effectiveness of existing security controls at the ground level to deal with the ransomware attacks. Auditor shall examine the effectiveness of people, process and technologies to deal with such attack considering both DC and DR have been impacted.
7. If for some reasons, auditors use the sample-based approach while performing the cyber security audit, following proposed criteria for sample examination must be adopted:
   1. For all critical assets (as defined by SEBI): 100 % samples shall be analyzed.
   2. For not so critical assets: more than 25 % and the selection should be based on relative importance, priority to newly added systems and randomness.
8. **Vulnerability Assessment and Penetration Testing (VAPT)**
9. VAPT should cover the entity’s Information system infrastructure which includes endpoints, user accounts, networking systems, security devices, servers, databases, applications systems accessible through WAN, LAN as well as with public IP’s, websites (irrespective of where hosted including their DR site)
10. Penetration Testing (PT) shall be done through all possible ingress and egress points/segments within the IT network (both internal and external) of entity.
11. Any IT asset and/or network physically and logically separate from the core network shall be considered excluded from the scope of VAPT.
12. Auditor should carry out an assessment of threat & vulnerabilities and assess the risks in entity’s Information Technology 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. Auditor shall perform the onsite assessment of the assets under the scope of this document.
13. It may also be noted that the VAPT shall include internal vulnerability assessment of infrastructure and applications (grey box), internal penetration testing of intranet and external penetration testing of internet/external facing IPs and applications.
14. **Minimum checks for Vulnerability Assessment and Penetration Testing are noted below:**

| **Sr. No** | **Name of the test** | **Description/indicative List of activities but not limited to** | **Internet/ Intranet** |
| --- | --- | --- | --- |
|  |  | **Penetration Testing** |  |
| 1 | **OSINT** | Gather entity’s domain  information using   1. Who is, 2. DNS queries etc. 3. **E-mail Harvesting** 4. **Check for leakage of passwords for compromised e-mails.** 5. **Historical Data analysis** 6. **Google Dorking.** 7. Dark Web. | Internet |
| 2 | **Network scanning** | Identify active hosts on a  network, for simulating attack and also for network security assessment using below  procedures but not limited to   * 1. Name server responses   2. Review the outer wall of the network.   3. Review tracks   4. Review information leaks   5. WAF Fingerprinting | Internet |
| 3 | **Port scanning** | Identify active ports on server port addresses   1. Error Checking 2. Enumerate Systems 3. Enumerating Ports 4. Verification of Various Protocol Responses 5. Verification of Packet Level Response | Internet |
| 4 | **Port sweep** | Scan multiple hosts for a  specific listening port for potential vulnerabilities | Internet |
| 5 | **System & OS fingerprinting** | Guess the system information i.e., type and version of OS etc. | Internet |
| 6 | **System identification and trusted system scanning** | Perform the system  identification & trusted system scanning which would include but not limited to the following   1. Identify server uptime to latest patch releases. 2. Match each open port to a service. 3. Identify the application behind the service and the patch level using banners or fingerprinting. 4. Verify the application on the system and the version. 5. Locate and identify service remapping or system redirects. 6. Identify the components of the listening service. 7. Use UDP-based service | Internet |
| 7 | **Web Application/ applications/ website penetration testing services** | Perform below listed penetration testing  services but not limited to:   1. Automated fuzzing. 2. Encryption usage testing (e.g., applications’ use of encryption) 3. Testing systems for user session management to see if unauthorized access can be permitted including but not limited to.    1. Input validation of login fields.    2. Cookie security.    3. Lockout testing.    4. User session integrity testing. 4. The solution partner shall perform the application penetration test Services on mobile applications of entities 5. Injection attacks. 6. Broken Authentication and Session Management. 7. Cross Site Scripting (“XSS”). 8. Secure direct object references 9. Security misconfiguration. 10. Sensitive data exposure. 11. Missing function level access control. 12. Cross Site Request Forgery (“CSRF”). 13. Using components with known vulnerabilities. 14. Invalidated redirects and forwards. 15. Review of specific controls against Web Defacing and uploading of Trojan/ Virus/ Malware/ Spyware etc. on various servers and further spread of the same to clients/connected machines. 16. LDAP injection 17. OWASP top 10 and SANS Top 25 CWE. | Internet / Intranet |
| 8 | **Network Penetration Testing Services** | Perform network penetration testing services  as listed below but not limited to:   1. The auditor should be able to identify network services exposed over entities system’s IP addresses. This should also be able to identify if the services blocked by network security solutions could also be exposed to internet. 2. Identify targets and map attack vectors (i.e., threat modelling). 3. Provide penetration testing from both inside and outside of Client’s network. 4. Internet Protocol (“IP”) address mapping of network devices. 5. Logical location mapping of network devices. 6. Transmission Control Protocol (“TCP”) scanning, connect scan, SYN scan, RST scan, User Datagram Protocol (“UDP”) scan, Internet Control Message Protocol (“ICMP”) scan, and Remote Procedure Call (“RPC”) port scan etc. 7. Operating System (“OS”) fingerprinting (OS fingerprinting is the combination of passive research and active scanning tools to generate an accurate network map). 8. Banner grabbing. 9. Brute force attacks. 10. Denial of Service (DOS) and Distributed Denial of Service (“DDoS”) testing. 11. Network sniffing. 12. Spoofing. 13. Trojan attacks | Internet and  Intranet |
| 9 | **Wireless Penetration Testing Services** | Perform wireless penetration testing as listed below but not limited to:   1. Wireless network testing / war driving. 2. / Wi-Fi cracking (WPA2 or WPA3). 3. Telephony or Voice over Internet Protocol (“VoIP”) testing, as requested |  |
| **Sr. No** | **Name of the test** | **Description/indicative List of activities but not limited to** | **Internet/ Intranet** |
|  |  | **Vulnerability Assessment** |  |
| 10 | **System identification on intranet** | Perform the system identification scanning which would include but not limited to the following in intranet   * 1. Obtain internal IP information about approved targets   2. In stealth mode perform a port sweep to develop a map of internal network structure and design   3. Attempt to identify critical business systems   4. Attempt to identify databases systems, web applications and other technologies based on footprint.   5. Scan multiple hosts for a specific listening port for potential vulnerabilities   6. Determine the system information i.e., type and version of OS etc. |  |
| 11 | **Vulnerability scanning** | Carry out vulnerability assessment for entire IT assets. Auditor shall conduct the research including but not limited to the following   1. Integrate the currently popular scanners,   latest scanning definitions/signatures, hacking tools, and exploits into the tests.   1. Measure against the currently popular scanning tools. 2. Determine vulnerability by system   and application type.   1. Match vulnerabilities to services. 2. Determine application type and service   by vulnerability.   1. Perform redundant testing with at least 2 automated vulnerability scanners. 2. Identify all vulnerabilities according to applications. 3. Identify all vulnerabilities according   to operating systems, servers,  network devices etc   1. Identify all vulnerabilities from similar or like systems that may also affect the 2. target systems 3. Verify all vulnerabilities found during the   scanning phase for false positives and  false negatives.   1. Verify all positives. 2. In addition to the above solution partner Vulnerability Testing and verification also. 3. Buffer overflow - Conduct buffer overflow   vulnerability assessment and identify vulnerabilities |  |
| 12 | **Malware scanning** | * 1. Comprehensive scanning required for existing hostile or intrusive software, including computer viruses, worms, Trojans, ransomware, spyware, adware, scareware, and other malicious programs.   2. Verify whether Endpoint Detection and Response (EDR) is installed/implemented and activated or not. |  |
| 13 | **Spoofing** | Assess the scope of potential spoofing attacks i.e., IP, ARP, DNS server spoofing Email spoofing etc. and other applicable ones in the entity's environment | Internet |
| 14 | **OS hardening assessment** | Carry out the assessment of OS hardening of entity’s servers as per Center for Internet Security (CIS) or customized CIS standards. | Intranet |
| 15 | **Denial Of Service (DoS) attacks and DDoS attacks** | Analyse the below listed  vulnerabilities but not limited to which may lead to DoS or DDoS attack   1. Check the exposure restrictions of systems to non-trusted networks. 2. Verify that baselines are established for normal system activity. 3. Verify what procedures are in place to respond to irregular activity. | Internet |
| 16 | **Authorization testing** | 1. Perform authorization & authentication testing for administrative accounts for the present AD /IDAM/ etc. systems. 2. Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege". 3. **Perform known attacks for AD abuse.** | Intranet |
| 17 | **Lockout testing** | Perform the brute force attack etc., lockout to identify any vulnerabilities | Internet |
| 18 | **Password cracking** | Perform Password cracking, cryptographic attacks etc. to check the vulnerabilities | Internet |
| 19 | **Cookie security and web bug analysis** | Review the cookie settings in all session management servers and identify the vulnerabilities | Intranet and internet |
| 20 | **Server and Database configuration assessment** | Review the present configuration of servers and recommend for the improvements | Intranet |
| 21 | **All network and security devices assessment** | * 1. Review the present configuration of network and security devices and recommend for the improvements.   2. Firewall rules review | Intranet and internet |
| 22 | **Website/web applications assessment** | Assess web applications and websites with and without credentials having different access levels like operator, supervisor, administrator, etc., to check for vulnerabilities like privilege escalation, input validation, etc. | Internet and Intranet |
| 22.a | **Broken Authentication and** **Session Management** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.b | **SQL injection** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.c | **Cross-Site Scripting** | Identify vulnerabilities  using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.d | **Insecure Direct Object References** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.e | **Sensitive Data Exposure** | Identify vulnerabilities  using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.f | **Missing Function Level Access** **Control** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.g | **Cross-Site Request Forgery** **(CSRF)** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.h | **Un-validated Redirects and** **Forwards** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.i | **Failure to Restrict URL Access** | Identify vulnerabilities  using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.j | **Insufficient Transport Layer Protection** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.k | **Any other vulnerability types, applicable to web applications** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet and Intranet |
| 22.l | **Web defacing and uploading of malware** | Review of specific controls against Web Defacing and uploading of Trojan/ Virus/ Malware/ Spyware etc. on various servers and further spread of the same to clients/connected machines | Internet and Intranet |
| 22 | **OWASP 10 web application vulnerabilities** | To review the applications against OWASP top 10 vulnerabilities as on the date of assessment and SANS Top 25 CWE. | Internet and Intranet |
| 23 | **IDS/IPS review and fine tuning of signatures** | Perform IDS/IPS review including but not limited to the following:   1. IPS and features identification 2. Testing IPS configuration 3. Reviewing IPS logs and alerts | Intranet |
| 24 | **Man in the Middle attack** | Perform man in the middle attack to identify sensitive data exposure vulnerability | Internet |
| 25 | **Man in the browser attack** | Perform man in the browser attack to identify sensitive data exposure vulnerability | Internet |
| 26 | **Directory Traversal** | Assess and identify the  directory travel vulnerabilities in entity’s systems | Internet |
| 27 | **Any other vulnerability associated with entity’s IT components** | Identify vulnerabilities using mix of automatic and manual assessment techniques | Internet & Intranet |
| 28 | **Cryptographic controls** | Identify vulnerabilities in  implementation of below technologies but not limited to   * 1. SSL configuration   2. Validate cryptographic strength | Internet |
| 29 | **DNS** | Scan DNS servers for finding below listed vulnerabilities but not limited to   * 1. Zone transfer   2. DOS and DDOS   3. Cache Poisoning etc. | Internet & Intranet |
| 30 | **Wireless Leak Tests** | Perform the vulnerability assessment & wireless leak test through below listed activities but not limited to   * + 1. Verify distance in which the wireless communication extends beyond the physical boundaries of the organization.     2. Verify authentication methods of the clients.     3. List equipment needed for testing.     4. Verify that encryption is configured and running - and what key length used.     5. Verify that clients can't be forced to fallback to plaintext mode.     6. Probe network for possible DoS problems     7. .     8. Controls for rogue access points | Intranet and physically should be present |
| 31 | **Internal Network Segmentation Testing and architecture review** | The auditor should evaluate Internal Network Segmentation Controls of the entity’s system. The auditor, thus has to identify the possibilities of unauthorized access from one Network Segment to another Network Segment. The auditor will be provided one testing from each network segment of the entity’s system to check for Internal Network Segmentation.  Network Architecture Review of various network zones including LAN, WAN, Wi-Fi etc. to identify any security vulnerabilities and suggest remedial measures |  |
| 32 | **Additional Penetration testing services** | Perform Penetration testing as provided below  but not limited to:   1. OWASP web application penetration testing methodologies 2. PCI standard penetration testing services (if existing) 3. Verify if the EDR / anti-malware services on servers and endpoints can be terminated through penetration testing tools. 4. On termination of EDR / anti-malware services, does it send any alert to SIEM or console at centralised location ? |  |
| 33 | **Black Box**  **Testing** | Entire IT infrastructure, applications, Databases, websites etc. |  |
| 34 | **Grey Box**  **Testing** | Entire applications, Databases, websites etc. |  |
| 35 | **Cloud**  **Infrastructure VAPT** | The auditor shall identify various attack vectors by delving deeply into the cloud architecture, which ranges from the network layer of the cloud design, access management, testing of cloud management interfaces to the cloud applications running on cloud data centres. The scope of audit/ VAPT should be limited to the components/ services managed by the Regulated Entities. In addition to above, the resources deployed for such cloud assessment should possess sufficient skills and expertise to detect the cloud specific risks (Ex.: multi-tenant isolation, cloud management interface security etc.). |  |

1. **Deliverables:**
   * + 1. Vulnerability Threat and Risk Analysis report.
       2. VA & PT report.
       3. Cyber Security Audit report.
       4. SOC efficacy report.
       5. Report of status of whitelisting approach adopted by entity.
       6. Compliance status against NCIIPC control guidelines
2. **Note:** Auditor should record its findings in detail, mentioning about the checks and methodology adopted by the auditor while performing audit. This should be supported by relevant documents/evidence, where required.