

# Vulnerability Assessment Checklist

Details of the Organization	
Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	
<i>Is Your Organization Subject to Any Specific Regulatory Requirements? (e.g., Sarbanes-Oxley, GLBA, HIPAA)</i>	

Details of the Incident Handler/Information Security Officer			
Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Job Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

**The following questions need to be answered before vulnerability assessment to estimate time as well as thoroughness of the assessment:**

Audit Information	
1. Does the organization require network-based vulnerability assessment?	
○ Specify the details of networks and hosts visible on the Internet that need thorough assessment	
2. Does the organization require host-based vulnerability assessment?	
○ Specify the details of host systems that need thorough assessment	
3. Does the organization require physical, compliance, or enterprise assessment?	
○ If compliance assessment required, which regulations need to be considered	
4. Does the organization require application vulnerability assessment?	
○ Specify the applications details (e.g., URL, application name, installer, etc.)	
○ Specify whether the application vulnerability assessment to be performed using user/administrator credentials or not	
5. Specify if any other details exist _____	
Network Security Information	
1. Has the organizational network ever been compromised (internally or externally)? Specify details of compromise	
2. List all the IP address blocks registered under the organization name	
3. List all the domain names registered under the organization name	

4. Does the organization has deployed local firewall systems?	
○ Specify the firewall details (list quantity and manufacturer/provider details)	
5. Does the organization has deployed local IDS systems?	
6. Does the organization has deployed local IPS systems?	
7. Does the organization use host-based IDS (HIDS) or network-based IDS (NIDS) or combination of both?	
○ Specify the IDS/IPS details (list quantity and manufacturer/provider details, include HIDS, NIDS, IPS systems)	
8. Does the organization use DMZ networks?	
9. Does the organization use Intranet/ Extranet networks (i.e., use any dedicated connections to other organization's networks (business partners, vendors, etc.))?	
○ Specify all the dedicated connections to other networks	
10. Does the organization provide/use any Remote Access services?	
○ Specify the type of remote access services used by the organization (e.g., VPN, Dial-up RAS, etc.)	
11. Does the organization use VPN tunneling between various sites?	
○ Specify the type and number of VPN tunnels in use	
12. Does the organization have any systems that use modems?	

<ul style="list-style-type: none"> <li>○ Specify the modem details (list quantity and manufacturer/provider details)</li> </ul>	
<p>13. Specify if any other details exist</p> <p>_____</p>	
<b>System Information</b>	
<p>1. How many Microsoft Windows Servers does the organization use?</p>	
<ul style="list-style-type: none"> <li>○ Specify the Windows servers details including quantity, hardware and software configuration</li> </ul>	
<p>2. How many Unix/Linux servers does the organization use?</p>	
<ul style="list-style-type: none"> <li>○ Specify the Unix/Linux server's details including specific distributions, quantity, hardware and software configuration</li> </ul>	
<p>3. List out the servers used by the organizations other than the listed above</p>	
<ul style="list-style-type: none"> <li>○ Specify the server details including quantity and hardware and software configuration</li> </ul>	
<p>4. Does the organization use any Enterprise Resource Planning (ERP) applications (e.g., SAP, Oracle JD, etc.)?</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each ERP application in use</li> </ul>	
<p>5. Does the organization use any E-commerce applications?</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each E-commerce application in use</li> </ul>	
<p>6. Does the organization use any database technologies (e.g., MySQL, Oracle, Microsoft SQL Server, etc.)?</p>	

<ul style="list-style-type: none"> <li>○ Specify the details of each database technology in use</li> </ul>	
<p>7. Specify if any other details exist</p> <p>_____</p>	
<b>Service Information</b>	
<p>1. What services does the organization expose to the Internet? (e.g., SSH, FTP, SMTP, etc.)</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each service exposed to the Internet</li> </ul>	
<p>2. What services does the organization expose to the internal network?</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each service exposed to the internal network</li> </ul>	
<p>3. What scripting languages does the organization use for the web services? (e.g., PHP, ASP.NET, Perl, Java, Ruby, etc.)</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each language in use</li> </ul>	
<p>4. Does the organization use any anti-virus applications?</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of each anti-virus application in use</li> </ul>	
<p>5. Does the organization implement anti-virus using client/server or standalone configuration?</p>	
<ul style="list-style-type: none"> <li>○ Specify the details of the configurations in use</li> </ul>	
<p>6. Specify if any other details exist</p> <p>_____</p>	
<b>Log Information</b>	
<p>1. What are the current existing logs for the IT infrastructure? (e.g., network logs, physical logs, etc.)</p>	
<ul style="list-style-type: none"> <li>○ Specify all the logs currently active and running</li> </ul>	

2. What are the retention policy for security logs?	
○ Specify the details of the retention policy	
3. What type of log backup strategy is used by the organization?	
○ Specify the frequency of backup in a day	
4. Specify if any other details exist _____	

### Other Details of the Vulnerability Assessment

Impact of the Assessment:	<input type="checkbox"/> <b>Low</b> <input type="checkbox"/> <b>Moderate</b> <input type="checkbox"/> <b>High</b> <input type="checkbox"/> <b>Critical</b>
Current Status:	
<i>Additional Information, if Any:</i>	

### Security Team Involved in the Assessment

Name	Title	Organization	Phone	Email

\_\_\_\_\_  
**Incident Handler's Signature**

\_\_\_\_\_  
**Date**