

<b>Audit Checklist #2 Security Issues for Oracle 9i RDMS</b>				
<b>STEP</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>	<b>COMMENTS/REFERENCES</b>
1. Has the entity installed only what is required? The Oracle9i pack contains a host of options and products in addition to the database server. Install additional products and options only as necessary.				
2. Has the entity locked and expired default user accounts? Oracle 9i installs with a number of default (preset) database server user accounts. If left open in their default status, these user accounts can be exploited to gain unauthorized access to data or disrupt database operations. Determine if the organization has taken steps to LOCK and EXPIRE all default database user accounts except SYS, SYSTEM, SCOTT, DBSNMP, OUTLN and the three JSERV database users. If any default database server user account other than the ones left open is required for any reason, a DBA need simply unlock and activate that account with a new, meaningful password.				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>3. Are default user passwords changed at time of installation? The most common method by which Oracle9i can be compromised is a default database server user account which still has a default password associated with it after installation.</p> <ul style="list-style-type: none"> <li>➤ <u>Administrative Users</u> - SYS installs with a default password of CHANGE_ON_INSTALL and SYSTEM installs with a default password of MANAGER. Determine if the organization has changed the default passwords associated with users SYS and SYSTEM immediately upon installation of the database server.</li> <li>➤ <u>All Users</u> – SCOTT installs with the default password TIGER; the three JSERV accounts (AURORASJIS\$UTILITY\$, AURORA\$ORB\$SUAUTHENTICATED AND OSE\$HTTP\$ADMIN each install with randomly-generated passwords. Each of the other accounts install with a default password that is exactly the same as that user account (e.g., user MDSYS installs with password MDSYS). Determine if the organization has changed these passwords immediately upon installation as well.</li> </ul>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>4. Does the organization strictly enforce password management? Basic password management rules (such as password length, history, complexity, etc.) as provided by the database be applied to all user passwords and that all users be required to change their passwords periodically.</p>				
<p>5. Has the organization enabled data dictionary protection? Oracle recommends that customers implement data dictionary protection to prevent users having the 'ANY' system privileges from using such privileges on the data dictionary. The entity does this by setting the init&lt;sid&gt;.ora (Oracle9i control file) configuration parameter, in the following manner: 07_DICTIONARY_ACCESSIBILITY = FALSE. By doing so, only those authorized users making DBA-privileged (e.g. CONNECT / AS SYSDBA) connections can use the 'ANY' system privilege on the data dictionary. However, if a user requires view access to the data dictionary, it is permissible for the entity to grant that user the SELECT ANY DICTIONARY system privilege.</p>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>6. Does the entity practice the principle of least privilege?</p> <ul style="list-style-type: none"> <li>➤ <u>Grant necessary privileges only</u> - Database users should be given only those privileges that are actually required to efficiently and succinctly perform his or her job. To implement least privilege, restrict: 1) the number of SYSTEM and OBJECT privileges granted to database users, and 2) the number of SYS-privileged connections to the database as much as possible. For example, there is generally no need to grant CREATE ANY TABLE to any non DBA-privileged user.</li> <li>➤ <u>Revoke unnecessary privileges from PUBLIC</u> – Revoke all unnecessary privileges and roles from the database server user group PUBLIC. PUBLIC acts as a default role granted to every user in an Oracle database. Any database user can exercise privileges that are granted to PUBLIC. Such privileges include EXECUTE on various PL/SQL packages that may permit a minimally privileged user to access and execute packages that he/she may not directly be permitted to access.</li> </ul>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>Other more powerful packages that may potentially be misused include:</p> <ul style="list-style-type: none"> <li>o UTL_SMTP – Permits arbitrary mail messages to be sent from one arbitrary user to another arbitrary user. Granting this package to PUBLIC may permit unauthorized exchange of mail messages.</li> <li>o UTL_TCP – Permits outgoing network connections to be established by the database server to any receiving (or waiting) network service. Thus, arbitrary data may be sent between the database server and any waiting network service.</li> <li>o UTL_HTTP – Allows the database server to request and retrieve data via HTTP. Granting this package to PUBLIC may permit data to be sent via HTML forms to a malicious web site.</li> <li>o UTL_FILE – If configured improperly, this package allows text level access to any file on the host operating system.</li> </ul>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>7. Does the entity effectively enforce access controls?</p> <ul style="list-style-type: none"> <li>➤ <u>Authenticate clients properly</u> – Remote authentication is a security feature provided by Oracle9i such that if turned on (TRUE), it defers authentication of users to the remote client connecting to an Oracle database. Thus, the database implicitly trusts any client to have authenticated itself properly. To restrict remote authentication and thereby defer client trust to the database, set the init&lt;sid&gt;.ora (Oracle9i control file) database configuration parameter in the following manner:  REMOTE_OS_AUTHENT = FALSE.</li> <li>➤ <u>Limit the number of operating system users</u> – Limit the number of users with operating system accounts (administrative, root-privileged or minimally privileged) on the Oracle9i host (physical machine) to the least number possible.</li> </ul>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>8. Has the entity taken the necessary steps to restrict network access?</p> <ul style="list-style-type: none"> <li>➤ <u>Utilize a firewall</u> – Keeping the database server behind a firewall.</li> <li>➤ <u>Never poke a hole through a firewall</u> – If Oracle9i is behind a firewall, do not, under any circumstances, poke a hole through the firewall. For example, do not leave open Oracle Listener’s 1521 port to make a connection to the Internet or vice versa.</li> <li>➤ <u>Prevent unauthorized administration of the Oracle Listener</u> – Always establish a meaningful, well-formed password for the Oracle Listener to prevent remote configuration of the Oracle Listener. Additionally, set the listener.ora (Oracle Listener control file) security configuration parameter in the following manner:</li> </ul> <p style="text-align: center;">ADMIN_RESTRICTIONS_listener_name = ON</p>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<ul style="list-style-type: none"> <li>➤ <u>Check network IP addresses</u> – Utilize the Oracle Net “valid node checking” security feature to allow or deny access or Oracle server processes from network clients with specified IP addresses. To use this feature, set the following protocol.ora (Oracle Net configuration file) parameters:   <ul style="list-style-type: none"> <li>Top.validnode_checking = YES</li> <li>Top.excluded_nodes = (list of IP addresses)</li> <li>Top. Invited_nodes = (list of IP addresses)</li> </ul> </li> <li>➤ <u>Encrypt network traffic</u> – Utilize Oracle Advanced Security to encrypt network traffic between clients, databases and application servers.</li> <li>➤ <u>Harden the operating system</u> – Harden the host operating system by disabling all unnecessary operating system services. Both UNIX and Windows platforms provide a variety of operating system services, most of which are not necessary for most deployments (e.g. FTP, TFTP, etc.).</li> </ul>				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
9. Has the entity implemented a policy of always applying all relevant and current security patches for both the operating system on which Oracle9i resides and Oracle9i itself? Periodically check the security site on Oracle Technology Network for details on security alerts released by Oracle Corporation.				