
# Center for Internet Security Benchmark for Oracle 9i/10g Ver. 2.0

## Table of Contents

**Agreed Terms of Use**

*Background*.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

*No representations, warranties and covenants*.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as availabel" without representations, warranties or covenants of any kind.

*User agreements*.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

1. No network, system, device, hardware, software or component can be made fully secure;

2. We are using the Products and the Recommendations solely at our own risk;

3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

*Grant of limited rights*.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

*Retention of intellectual property rights; limitations on distribution*.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations (“**CIS Parties**”) harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS’s right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

*Special rules*.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

*Choice of law; jurisdiction; venue*.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

**Introduction**

This provisional document is derived from research conducted utilizing the Oracle 10g program, the Oracle's Technology Network (otn.oracle.com), various published books and the Oracle 9i Database baseline document. The provisional status is based on the lack of sufficient informational resources for this newly released application. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an Oracle 10g database environment. Targeted for newly established and/or deployed Oracle 10g database in Unix or Windows operating system platforms, it is for the use of DOE advanced Oracle Database Administrators. With the use of the settings and procedures in this document, an Oracle database may be secured from conventional "out of the box" threats. Recognizing the nature of security cannot and should not be limited to only the application, the scope of this document is not limited to only Oracle specific settings or configurations, but also addresses backups, archive logs, "best practices" processes and procedures that are applicable to general software and hardware security.

New to the 10g baseline document is organization into chapters based on logical groupings. Within chapters, items are organized by level. All items function on layer 7, the Application layer of the OSI model, or, as in the case of many policy items, are not applicable to the OSI model. Therefore, groupings via the OSI model would not be relevant.

Applicable items were verified and tested against an Oracle 10g default install on both a default Windows 2000 Server and a Solaris 9 Unix machine. The Oracle version used was 10.0.1.2 install disks, patched up to 10.0.1.3. Where the default setting is less secure then the recommended setting a caution has been provided in the comment section below the separator bar or as a note below a chapter heading. Default installs for both the operating system and the database may differ dependent on versions and options installed so this is to be used as a general guide only. Unix settings should translate to other varieties of Unix, but were only tested against Solaris 9. If any differences are found, please contact the CIS team.

This document is not intended as a guidance document. It is the minimum required means of diligence for the protection of an Oracle 10g database. For issues of guidance, the NSA guideline web site (http://www.nsa.gov/snac) and the DOE guideline resources web site (http://www.cisecurity.org/bench_oracle.html) each provide excellent guidance documents for both operating systems and specific applications.

Under the Level heading, scoring data has been temporarily included:
S – To be scored.
N – Not to be scored.
R – Reportable, but not to be scored.
This data, as well as this paragraph should be deleted when no longer necessary.

## 1. Operating System Specific Settings

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 1.01 | Windows platform | Do not install Oracle on a domain controller | Oracle must only be installed on a domain member server or a standalone server. | 10g,9i | √ | | 1 |
| 1.02 | Windows Services | Disable or remove unnecessary Windows services. | Refer to Appendix B for which Windows 2000 Services must be disabled. | 10g,9i | √ | | 1 |
| 1.03 | Windows Networking | Remove all unnecessary protocol stacks except TCP/IP. | Have only TCP/IP available. | 10g,9i | √ | | 1 |
| 1.04 | Windows Administrator's Account | Rename the local computer's Administrator account | Do not use the default name. | 10g,9i | √ | | 1 |
| 1.05 | Windows Oracle Account | Use local administrator account | Run the Oracle services using a local administrator account created specifically for Oracle. Use the account created to install the product. Deny log on locally to this account. | 10g,9i | √ | | 1 |
| 1.06 | Windows Oracle Domain Account | Use restricted service account (RSA) | If the Oracle services require domain resources, then the server must be a domain server and the Oracle services must be run using a restricted service account (RSA), i.e., restricted domain user account. It must be added to the local administrators group on the server running the Oracle services. | 10g,9i | √ | | 1 |
| 1.07 | Windows Oracle Domain Global Group | Create a global group for the RSA and make it the RSA's primary group | The RSA account is not an account that should have access to resources that all domain users have a need to access. Note: Do not assign any rights to the group. | 10g,9i | √ | | 1 |
| 1.08 | Windows Oracle Account Domain Users Group Membership | Remove the RSA from the Domain Users group | The RSA must have limited access requirements. | 10g,9i | √ | | 1 |
| 1.09 | Windows Oracle Domain Network Resource Permissions | Verify and set permissions as needed | Give the appropriate permissions to the RSA or global group for the network resources that are required. The RSA must have limited access requirements. | 10g,9i | √ | | 1 |
| 1.10 | Windows Oracle Domain Account Logon to… Value | Limit to machine running Oracle services | Configure the RSA to only log on to the computer that is running the Oracle services and on the actual computer deny the right to log on locally as the RSA. | 10g,9i | √ | | 1 |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 1.11 | Windows Local Users Group Membership | Remove Domain Users from Users group | If the server is a domain server, then remove the Domain Users group from the local computer's Users group. | 10g,9i | √ | | 1 |
| 1.12 | Windows Directory Permissions | Verify and set permissions as needed | Remove the Everyone Group from the installation drive or partition and give System and local Administrators Full Control. | 10g,9i | √ | | 1 |
| 1.13 | Windows Program Folder Permissions | Verify and set permissions as needed | Remove permissions for the Users group from the [OS drive]:\Program Files\Oracle folder. The Oracle program installation folder must allow only limited access. | 10g,9i | √ | | 1 |
| 1.14 | Windows Tools Permissions | Verify and set permissions as needed | Tighten the permission on tools (*.exe) in the WINNT and System32 folders, e.g., only Administrators should have permissions on these files; however, deny access to the Oracle service account. The Oracle service account is an administrator account, but also must be denied access to executables. | 10g,9i | √ | | 1 |
| 1.15 | Windows HKLM Registry Key Permissions | Remove the Everyone group on the HKLM key. | The Everyone group must not be able review registry settings. | 10g,9i | √ | | 1 |
| 1.16 | Windows Oracle Registry Key Permissions | Verify and set permissions as needed | Give Full Control over the HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE key to the account that will run the Oracle services and remove the local Users group if it's not required. Give read permissions to those users that require it. Access to the Oracle registry key must be limited to those users that require it. | 10g,9i | √ | | 1 |
| 1.17 | Windows Oracle Registry Key Setting | Set OSAUTH_ PREFIX_DOMAIN registry value to TRUE | This registry value must be created or updated in HKEY_LOCAL_MACHINE\ SOFTWARE\ORACLE\ALL_HOMES | 10g,9i | √ | | 1 |
| 1.18 | Windows registry | use_shared_socket=TRUE | Add this to the HKEY_LOCAL_MACHINE\ SOFTWARE\ORACLE\HOME<#> registry key if random port reassignment is undesired, such as if there is a need to pipe through a firewall. See Oracle Metalink note 124140.1 for details. | 10g,9i | √ | | 2 |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 1.19 | Oracle software owner host account | Lock account | On Unix systems, lock the Oracle software owner account. If the account cannot be locked, use a very strong password for the account. Account can be unlocked if system maintenance is required. This is not recommended for Windows environments. | 10g,9i | | √ | 2 |
| 1.20 | All associated application files | Verify permissions | Check the file permissions for all application files for proper ownership and minimal file permissions. This includes all 3rd party application files on the server that access the database. Any 3rd party applications must be installed on a separate server from the database. If this is not possible in the environment, ensure that the 3rd party applications are installed on separate partitions from the Oracle software and associated datafiles. | 10g,9i | √ | √ | 2 |

## 2. Installation and Patch

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 2.01 | Installation | Try to ensure that no other users are connected while installing Oracle 10g. | The Oracle 10g installer application could potentially create files in a temporary directory with public privileges. It would be possible for any local user to delete, overwrite or corrupt these files during the installation process. Try to ensure that no other users are connected while installing Oracle 10g. Also set the $TMP and $TMPDIR environment variables to a protected directory with access given only to the Oracle software owner and the ORA_INSTALL group. | 10g | √ | √ | 1 |
| 2.02 | Version/Patches | Ensure the latest version of Oracle software is being used, and that the latest patches from Oracle Metalink have been applied. | It would be counterproductive to state specific version and patch levels in this document. Since they change on a regular basis, the version stated in here might be outdated by the time this document is being used. Check Oracle's site to ensure the latest versions: http://www.oracle.com/technology/software/index.html and latest patches: http://metalink.oracle.com/metalink/plsql/ml2_gui.startup | 10g,9i | √ | √ | 1 |
| 2.03 | tkprof | Remove from system | The tkprof utility must be removed from production environments. If tkprof must remain on the production system, it must be protected. Set file permissions of 0750 or less on Unix systems. On Windows systems, restrict access to only those users requiring access and verify that "Everyone" does not have access.<br>By default tkprof is installed. Be aware, default permissions are set as:<br>Windows: Default is sufficient | 10g,9i | √ | √ | 1<br>S |
| 2.04 | listener.ora | Change default name of listener | The listener must not be called by the default name. A distinct name must be selected. | 10g,9i | √ | √ | 1<br>S |
| 2.05 | listener.ora | Use IP addresses rather than hostnames | IP addresses instead of host names in the listener.ora file must be used.<br>Host names are used by default. | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 2.06 | otrace | Disable | Go to the $ORACLE_HOME/otrace/admin directory of your instance and remove or delete the dat files related to otrace. Do this for all *.dat files in this directory.<br>Note that this directory is installed for the Enterprise Manager Grid Controller. It is not installed with a default 10g database installation. | 10g,9i | √ | √ | 1<br><br>S |
| 2.07 | Listener password | Encrypt the Listener Password | Set an encrypted password for the listener. By default, the listener password is not set. | 9i | √ | √ | 1<br>S |
| | | Use Integrated Authentication | By default, the listener uses integrated authentication for Administrators (Windows), root (Unix), and the process owner. If additional users require access, set an encrypted password for the listener. | 10g | | | |
| 2.08 | Default Accounts (created by Oracle) | The following actions are recommended in order of preference for default accounts:<br>1. Drop the user<br>2. Lock the user account<br>3. Change the default password | Depending on the Oracle version specific environment, on the default accounts either drop the user, lock the user account, or change the default password. | 10g,9i | √ | √ | 2<br><br>S |
| 2.09 | OEM objects | Remove if OEM not used (see comments) | Execute $ORACLE_HOME/rdbms/admin/ catnsnmp.sql to remove all the objects and delete the file $ORACLE_HOME/bin/dbsnmp. NOTE: database statistics will be unavailable in Enterprise Manager if this is set. | 10g,9i | √ | √ | 2<br><br>S |
| 2.10 | listener.ora | Change standard ports | Standard ports are well known and can be used by attackers to verify applications running on a server. | 10g,9i | √ | √ | 2<br><br>S |
| 2.11 | Third party default passwords | Set all default account passwords to non-default strong passwords | When installed, some third party applications create well-known default accounts in an Oracle database. The default password for these accounts must be changed or the account must be locked. | 10g,9i | √ | √ | 2<br><br>S |
| 2.12 | Service or SID name | Non-default | Do not use the default SID or service name of ORCL. | 10g,9i | √ | √ | 1 S |
| 2.13 | Oracle Installation | Oracle software owner account name NOT ‘oracle’ | Do not name the Oracle software owner account ‘oracle’ as it is very well known. | 10g,9i | √ | √ | 2<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 2.14 | Oracle Installation | Separate users for different components of Oracle | For Unix systems, create unique user accounts for each Oracle process/service in order to differentiate accountability and file access controls. The user for the intelligent agent, the listener, and the database must be separated. This is not recommended for Windows environments. | 10g,9i | | √ | 2 |

## 3. Oracle Directory and File Permissions

Note: The Oracle software owner in Windows is the account used to install the product. This account must be a member of the local Administrators group. The Windows System account is granted access to Oracle files/directories/registry keys. This account is not restated in the comments section below, but must not be removed. Removal of the System account will cause Oracle to stop functioning.

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 3.01 | Files in $ORACLE_HOME/bin | Verify and set ownership | All files in the $ORACLE_HOME/bin must be owned by the Oracle software account. In Windows, this account must be part of the Administrators group. | 10g,9i | √ | √ | 1 S |
| 3.02 | Files in $ORACLE_HOME/bin | Permissions set to 0755 or less on Unix systems | All files in the $ORACLE_HOME/bin directory must have permissions set to 0755 or less. | 10g,9i | | √ | 1 S |
| 3.03 | Files in $ORACLE_HOME (not including $ORACLE_HOME/bin) | Permissions set to 0750 or less on Unix systems | All files in $ORACLE_HOME directories (except for $ORACLE_HOME/bin) must have permission set to 0750 or less. | 10g,9i | | √ | 1 S |
| 3.04 | Oracle account .profile file | Unix systems umask 022 | Ensure the umask value is 022 for the owner of the Oracle software before installing Oracle.<br>Regardless of where the umask is set, umask must be set to 022 before installing Oracle. | 10g,9i | | √ | 1 |
| 3.05 | init.ora | Verify and restrict as needed permissions | File permissions must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1 S |
| 3.06 | spfile.ora | Verify and restrict as needed permissions | File permissions must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1 S |
| 3.07 | Database datafiles | Verify and restrict as needed permissions | File permissions must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1 S |
| 3.08 | init.ora | Verify permissions of file referenced by ifile parameter | If the ifile functionality is used, the file permissions of the referenced ifile must be restricted to the Oracle software owner and the dba group. | 10g,9i | √ | √ | 1 S |
| 3.09 | init.ora | audit_file_dest parameter settings | The destination for the audit file must be set to a valid directory owned by oracle and set with owner read/write permissions only. | 10g,9i | √ | √ | 1 S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 3.10 | init.ora | user_dump_dest parameter settings | The destination for the user dump must be set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.11 | init.ora | background_dump_dest parameter settings | The destination for the background_dump must be set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.12 | init.ora | core_dump_dest parameter settings | The destination for the core_dump must be set to a valid directory with permissions restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.13 | init.ora | control_files parameter settings | The permissions must be restricted to only the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.14 | init.ora | log_archive_dest _n parameter settings | File permissions must be restricted to the owner of the Oracle software and the dba group. For complex configurations where different groups need access to the directory, access control lists must be used. Note: If Oracle Enterprise Edition is installed, and no log_archive_dest_n parameters are set, the deprecated form of log_archive_dest must be used.<br>Default is " " (A null string) for all. Must configure and set paths, then ensure those directories are secure. | 10g,9i | √ | √ | 1<br>S |
| 3.15 | Files in $ORACLE_HOME/ network/admin directory | Verify and set permissions as needed | Permissions for all files must be restricted to the owner of the Oracle software and the dba group. Note: If an application that requires access to the database is also installed on the database server, the user the application runs as must have read access to the tnsnames.ora and sqlnet.ora files. | 10g,9i | √ | √ | 1<br>S |
| 3.16 | webcache.xml | Verify and set permissions as needed | File permissions must be restricted to the owner of the Oracle software and the dba group.<br>Installed with Enterprise Manager Grid Control software. | 10g,9i | √ | √ | 1<br>S |
| 3.17 | snmp_ro.ora | Verify and set permissions as needed | File permissions must be restricted to the owner of the Oracle software and the dba group.<br>Not installed in default installation. | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 3.18 | snmp_rw.ora | Verify and set permissions as needed | File permissions must be restricted to the owner of the Oracle software and the dba group.<br>Not installed in default installation. | 10g,9i | √ | √ | 1<br>S |
| 3.19 | sqlnet.ora | Verify and set permissions as needed with read permissions for everyone. | The sqlnet.ora contains the configuration files for the communication between the user and the server including the level of required encryption. | 10g,9i | √ | √ | 1<br>S |
| 3.20 | sqlnet.ora | log_directory_client parameter settings | The log_directory_client must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. | 10g,9i | √ | √ | 1<br>S |
| 3.21 | sqlnet.ora | log_directory_server parameter settings | The log_directory_server must be set to a valid directory owned by the Oracle account and set with owner and group read/write permissions only.<br>By default this is not set. | 10g,9i | √ | √ | 1<br>S |
| 3.22 | sqlnet.ora | trace_directory_client parameter settings | The trace_directory_client parameter settings must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. Be aware, this is usually set to $ORACLE_HOME/network/trace, with permissions set as: | 10g,9i | √ | √ | 1<br>S |
| 3.23 | sqlnet.ora | trace_directory_server parameter settings | The trace_directory_server must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. Be aware, this is usually set to $ORACLE_HOME/network/trace, with permissions set as: | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 3.24 | listener.ora | Verify and set permissions as needed | File permissions must be restricted to the owner of the Oracle software and the dba group. If backup copies of the listener.ora file are created these backup files must be removed or they must have their permissions restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.25 | listener.ora | log_file_listener parameter settings | The log_file_listener file must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. Be aware, this is usually set to $ORACLE_HOME/network/log/listener.log, with permissions set as: | 10g,9i | √ | √ | 1<br>S |
| 3.26 | listener.ora | trace_directory_*listener_name* parameter settings | The trace_directory_listener_name must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. Be aware, this is usually set to $ORACLE_HOME/network/trace, with permissions set as: | 10g,9i | √ | √ | 1<br>S |
| 3.27 | listener.ora | trace_file_*listener_name* parameter settings | This file must be owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.<br>By default this is not set. Be aware, this is usually set to $ORACLE_HOME/network/trace, with permissions set as: | 10g,9i | √ | √ | 1<br>S |
| 3.28 | sqlplus | Verify and set permissions as needed. | The permissions of the binaries for sqlplus on the server must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1<br>S |
| 3.29 | htaccess | Verify and set permissions as needed. | File permissions must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1 |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 3.30 | wdbsvr.app | Verify and set permissions as needed. | File permissions must be restricted to the owner of the Oracle software and the dba group. | 9i | √ | √ | 1 S |
| 3.31 | xsqlconfig.xml | Verify and set permissions as needed. | File permissions must be restricted to the owner of the Oracle software and the dba group. | 10g,9i | √ | √ | 1 S |

## 4. Oracle Parameter Settings

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 4.01 | init.ora | _trace_files_public= FALSE | Prevents users from having the ability to read trace files.<br>Default is FALSE. | 10g,9i | √ | √ | 1<br>S |
| 4.02 | init.ora | global_names= TRUE | Ensures that Oracle will check that the name of a database link is the same as that of the remote database.<br>Default is FALSE. | 10g,9i | √ | √ | 1<br>S |
| 4.03 | init.ora | max_enabled_roles=30 | This must be limited as much as possible. Typically SYS gets 20 roles by default.<br>Default is 150. | 10g,9i | √ | √ | 1<br>S |
| 4.04 | init.ora | remote_os_authent= FALSE | Connection without a password must be prevented.<br>Default is FALSE. | 10g,9i | √ | √ | 1<br>S |
| 4.05 | init.ora | remote_os_roles= FALSE | Connection spoofing must be prevented.<br>Default is FALSE. | 10g,9i | √ | √ | 1<br>S |
| 4.06 | init.ora | remote_listener=“ “ (A null string) | Prevent the use of a listener on a remote machine separate from the database instance.<br>Default is “ “ (A null string) NOTE: the field should be left empty. A space is not a null string. | 10g,9i | √ | √ | 1<br>S |
| 4.07 | init.ora | Audit_trail parameter set to OS, DB, or TRUE | Ensures that basic audit features are used. Recommend setting audit_trail to OS as it reduces the likelihood of a Denial of Service attack and it is easier to secure the audit trail. OS is required if the auditor is distinct from the DBA. Any auditing information stored in the database is viewable and modifiable by the DBA. Even with the AUDIT_TRAIL value set to FALSE, an audit session will report, "Audit succeeded."<br>Default=NONE. | 10g,9i | √ | √ | 1<br>S |
| 4.08 | init.ora | os_authent_prefix=“ “ (A null string) | It must be set to limit the external use of an account to an IDENTIFIED EXTERNALLY specified user.<br>Default is set to OPS$, which is for backward compatibility to previous versions. Null is recommended. | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 4.09 | init.ora | os_roles=FALSE | O/S roles are subject to control outside the database. The duties and responsibilities of DBAs and system administrators must be separated.<br>Default is FALSE. | 10g,9i | √ | √ | 1<br>S |
| 4.10 | init.ora | Avoid using utl_file_dir parameters | Do not use the utl_file_dir parameter. Specify directories using CREATE DIRECTORY.<br>Default is not to have it set. | 10g,9i | √ | √ | 1<br>S |
| 4.11 | init.ora | Establish redundant physically separate locations for redo log files. Use "LOG_ARCHIVE_DUPLEX_DEST" to establish a redundant location for the redo logs. | Redundancy for the redo logs can prevent catastrophic loss in the event of a single physical drive failure. If this parameter is used, it must be set to a valid directory owned by oracle set with owner and group read/write permissions only. For complex configurations where different groups need access to the directory, access control lists must be used.<br>Default is " " (A null string). Not set up by default. | 10g,9i | √ | √ | 1<br>S |
| 4.12 | init.ora | Specify redo logging must be successful. Use "LOG_ARCHIVE_MIN_SUCCEED_DEST" to ensure the successful logging of the redo files. | Specifying that the logging must succeed in one or more locations ensures redundancy of the redo logs.<br>Default is 1 | 10g,9i | √ | √ | 1<br>S |
| 4.13 | init.ora | sql92_security= TRUE | Enforce the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table.<br>Default is FALSE | 10g,9i | √ | √ | 1<br>S |
| 4.14 | listener.ora | admin_restrictions_*listener_name*=on | Replace *listener_name* with the actual name of your listener(s) for this parameter setting.<br>Not set and turned off by default. | 10g,9i | √ | √ | 1<br>S |
| 4.15 | listener.ora | logging_listener=ON | This must remain set to ON.<br>Not set, but turned on by default. | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 4.16 | Data logs | Use “ARCHIVELOG” mode for data logs by the command “ALTER DATABASE ARCHIVELOG”. | Prior to 10g log files were not archived automatically and required the setting “LOG_ARCHIVE_START=TRUE”, which has been deprecated in 10g.<br>Windows Event Logs and Unix System logs must be regularly monitored for errors related to the Oracle database.<br>While deprecated, setting still exists. | 10g,9i | √ | √ | 1<br>S |
| 4.17 | SQL key word “NOLOGGING” | Be aware of the potential for malicious code that can be performed without an audit trail under the key word “NOLOGGING”. | Note that “UNRECOVERABLE”, which was replaced by “NOLOGGING” is no longer supported in 10g. | 10g, 9i | √ | √ | 1<br>S |
| 4.18 | init.ora | o7_dictionary_ accessibility= FALSE | Prevents users or roles granted SELECT ANY TABLE from accessing the data dictionary.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.19 | init.ora | Remove the following line from the init.ora or spfile: dispatcher= (PROTOCOL= TCP) (SERVICE= <oracle_sid>XDB) | This will disable default ports ftp: 2100 and http: 8080 which are configured in the default installation starting with Oracle 9iR2.<br>By default this is set in the spfile in 10g and 9i. | 10g,9i | √ | √ | 2<br>S |
| 4.20 | Init.ora | AUDIT_SYS_OPERATIONS =TRUE | Auditing of the users authenticated as the SYSDBA or the SYSOPER provides an oversight of the most privileged of users.<br>Note: It is important that the database user should not have access to the system directories where the audits will be recorded. Ensure this by setting the AUDIT_SYS_OPERATIONS to TRUE.<br>Default is FALSE. Set in spfile. Set AUDIT_FILE DEST to where you want the logs to be.<br>Windows: Default is Event Viewer log file<br>Unix: Default is $ORACLE_HOME/rdbms/audit | 10g,9i | √ | √ | 2<br>S |
| 4.21 | listener.ora | inbound_connect_ timeout_*listener*=2 | Suggestion is to set to a low initial value and adjust upward if normal clients are unable to connect within the time allocated.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 4.22 | sqlnet.ora | tcp.validnode_ checking= YES | Set this parameter in the $ORACLE_HOME/network/admin/sqlnet.ora file.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.23 | sqlnet.ora | Set tcp.invited_nodes to valid values | Use IP addresses of authorized hosts to set this parameter in the sqlnet.ora file.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.24 | sqlnet.ora | Set tcp.excluded_nodes to valid values | Use IP addresses of unauthorized hosts to set this parameter in the sqlnet.ora file. Note: if the tcp.invited_nodes is set, the tcp.excluded_nodes values are ignored.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.25 | sqlnet.ora | sqlnet.inbound_ connect_timeout=3 | Suggestion is to set to a low initial value and adjust upward if normal clients are unable to connect within the time allocated.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.26 | sqlnet.ora | sqlnet.expire_time= 10 | If this is not set in the sqlnet.ora file, the default is never to expire.<br>Not set by default. | 10g,9i | √ | √ | 2<br>S |
| 4.27 | Accounts | Lock account access for application schema owners | Lock the account for the application schema owner. Users must not connect to the database as the application owner. | 10g,9i | √ | √ | 2<br>S |
| 4.28 | init.ora | remote_login_passwordfile=none | See tables below for detailed configuration recommendations. | 10g,9i | √ | √ | 2<br>S |
| 4.29 | $ORACLE_HOME/ bin/extproc | Remove binary from host | If extproc functionality is not required, remove this binary. If extproc functionality is required, refer to Oracle Metalink Security Alert 57 (244523.1) for instructions on securing extproc. | 9i | √ | √ | 2<br>S |
| 4.30 | tnsnames.ora | Remove extproc entry | If extproc functionality is not required, remove this entry. If extproc functionality is required, refer to Oracle Metalink Security Alert 57 (244523.1) for instructions on securing extproc. | 9i | √ | √ | 2<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 4.31 | listener.ora | Remove extproc entry | ExtProc functionality allows external C and Java functions to be called from within PL/SQL. If extproc functionality is not required, remove this entry. If extproc functionality is required, refer to Oracle Metalink Security Alert 57 (244523.1) for instructions on securing extproc. In short, create a new listener specifically for extproc. This listener must run as an unprivileged OS user. | 9i | √ | √ | 2<br><br>S |

## 5. Encryption Specific Settings

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 5.01 | OAS - General | Review requirement for integrity and confidentiality requirements. | Only implement OAS if a local integrity/encryption policy does not already exist, e.g., IPSec or other means for providing integrity/confidentiality services. | 10g,9i* | √ | √ | 2<br>S |
| 5.02 | OAS – Encryption Type | SQLNET.ENCRYPTION_SERVER=REQUIRED | This ensures that regardless of the settings on the user, if communication takes place it must be encrypted. | 10g,9i* | √ | √ | 2<br>S |
| 5.03 | OAS – Encryption Type | SQLNET.ENCRYPTION_CLIENT=(ACCEPTED\|REQUESTED\|REQUIRED) | Communication is only possible on the basis of an agreement between the client and the server regarding the connection encryption. To ensure encrypted communciation, set the value to “REQUIRED.”<br>With the server set to “REQUIRED” the client must match the encryption for valid communcation to take place.<br>NOTE: failure to specify one of the values will result in an error when an attempt is made to connect to a FIPS 140-1 compliant server. | 10g,9i* | √ | √ | 2<br>S |
| 5.04 | OAS – Encryption Seed | SQLNET.CRYPTO_SEED=some70charValue | Where possible use the maximum seed value (70 characters). Please be aware that in 9i and early version of 10g, the CRYPTO_SEED does not take the following characters: single quote(‘), double quote(“), space, number sign(#), equal sign(=), right or left paranthesis ((()), comma(,), or backslash(\).<br><br>Please see Metalink article 281928.1 for more information. | 10g,9i* | √ | √ | 2<br>S |
| 5.05 | OAS – FIPS Compliance | SQLNET.FIPS_140=TRUE | For FIPS 140-1 compliance, the FIPS value must be set to “TRUE.” The default value for this setting is “FALSE.”<br>NOTE: This value is not settable using the Oracle Net Manager. To set this value you must use a text editor and modify the sqlnet.ora file. | 10g,9i* | √ | √ | 2<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 5.06 | OAS – Encryption Method (FIPS 140) | SQLNET.ENCRYPTION_TYPES_SERVER=(DES\|DES40) | To satisfy the FIPS 140-1 criterion in Oracle, only DES or DES40 may be used and there must be an agreement between the SERVER and the CLIENT.<br>NOTE: These encryption standards do not meet the newer FIPS 140-2 standard. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.07 | OAS – Encryption Methods | In decending order of preference encryption keys for both client and server must be set to the maximum feasible value.<br><br>Example:<br>“sqlnet.encryption_types_server =(RC4_256, AES256, AES192)”<br><br>“sqlnet.encryption_types_client= (RC4_256, AES256, AES192)”<br><br>Availabel values with =>128 bit key encryption include:<br>RC4 256 bit key - RC4_256<br>AES 256 bit key - AES256<br>AES 192 bit key- AES192<br>3 Key Triple DES 168 bit effective key size - 3DES168<br>RC4 128 bit key- RC4_128<br>AES 128 bit key - AES128<br><br>Availabel values with less than 128 bit key encryption include:<br>2 Key Triple DES 112 bit effective key size - 3DES112<br>RC4 56 bit key - RC4_56<br>1 Key DES 56 bit effective key size - DES<br>RC4 40 bit key - RC4_40<br>DES40 40 bit effective key size - DES40 | At a minimum, use 128 bit key encryption.<br>Note: There are publicly availabel attacks that allow a Pentium III to crack 40 and 56 bit key encryptions. Encryption below 128 bit keys should be considered minimally effective.<br><br>Unfortunately without the use of a third party encryption method, with the FIPS value set to TRUE, only DES and DES40 are allowed as legal values. This sets the database to the standard of FIPS140-1 and not to the standard of FIPS140-2.<br><br>For more information about FIPS 140-2 issues, please see Appendix C. | 10g,9i* | √ | √ | 2<br><br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 5.08 | OAS – Integrity Protection | Integrity check for communication between the server and the client must be established.<br><br>"SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED"<br><br>"SQLNET.CRYPTO_CHECKSUM_CLIENT=REQUIRED" | The integrity check for communication can prevent data modifications. Two check sum algorithms are availabel; SHA-1 and MD5.<br><br>Oracle's implementation of this setting also offers protection against replay attacks.<br><br>Reference Oracle Metalink 76637 for more information. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.09 | OAS – Integrity Protection | Set SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA1) | If possible, use SHA1 instead of MD5. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.10 | OAS – Oracle Wallet Owner Permissions | Set configuration method for Oracle Wallet. Ensure only the appropriate Oracle user account has access to the wallet. | The Oracle service account must have access to the wallet. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.11 | OAS – Oracle Wallet Trusted Certificates | Remove certificate authorities (CAs) that are not required. | Trust only those CAs that are required by clients and servers. | 10g,9i* | √ | √ | 2<br>S |
| 5.12 | OAS – Oracle Wallet Trusted Certificates Import | When adding CAs, verify fingerprint of CA certificates. | When adding CA certificates via out-of-band methods, use fingerprints to verify the certificate. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.13 | OAS – Certificate Request Key Size | Request the maximum key size availabel. | Select the largest key size availabel that is compatible with the network environment. | 10g,9i* | √ | √ | 2<br>S |
| 5.14 | OAS – Server Oracle Wallet Auto Login | Allow Auto Login for the server's Oracle Wallet | For Windows Oracle database servers, SSL will not work unless Auto Login is set. | 10g,9i* | √ | √ | 2<br>S |
| 5.15 | OAS – SSL Tab | SSL is preferred method. If PKI not possible, use OAS Integrity/Encryption. | OAS Integrity/Encryption should only be used if required because of non-SSL clients. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.16 | OAS – SSL Version | Set SSL version.<br>SSL_VERSION = 3.0 | Do not set this parameter with "Any". | 10g,9i* | √ | √ | 2<br>S |
| 5.17 | OAS – SSL Cipher Suite | Set SSL Cipher Suite.<br>SSL_CIPHER_ SUITES = SSL_ RSA_ WITH_3DES_ EDE_ CBC_SHA) | At a minimum, triple DES should be supported. Add SSL_RSA_WITH_RC4_128_SHA or SSL_RSA_WITH_RC4_128_MD5 only if clients don't support the recommended value. | 10g,9i* | √ | √ | 2<br><br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 5.18 | OAS – SSL Client DN Match | Set tnsnames file to include SSL_SERVER_ CERT_DN parameter with the distinguished name (DN) of the certificate. | This will reduce possibility of certificate masquerading. | 10g,9i* | √ | √ | 2<br><br>S |
| 5.19 | OAS – SSL Client Authentication | SSL_CLIENT_ AUTHENTICATION=TRUE | If client certificates are not supported in the enterprise, then set to FALSE. | 10g,9i* | √ | √ | 2<br>S |
| 5.20 | OAS – Encryption Tab | Use OAS encryption only if SSL is not feasible. | OAS Integrity/Encryption should only be used if required because of non-SSL clients. | 10g,9i* | √ | √ | 2<br>S |
| 5.21 | Encryption | Where possible, use a procedure that employs a content data element as the encryption key that is unique for each record. | By employing a procedure that uses data elements that change for each record the resulting ciphertext will be unique. As an example if the same value, key, and encryption are used for a value in a record the resulting ciphertext will be identical. Someone knowing the value of one of the records independent of the ciphertext can by inference know the value of other records that display the same ciphertext. | 10g,9i | √ | √ | 2<br><br>S |
| 5.22 | Encryption | Use RAW or BLOB for the storage of encrypted data. | Storing data in CLOB may result in a failure in decryption if the same number letter symbol set is not used. The use of RAW or BLOBs prevents this error and preserves the data. | 10g,9i | √ | √ | 2<br><br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 5.23 | Encryption | Use a virtual private database (VPD) to protect rows by implementing Oracle Label Security(OLS).<br><br>If keys are stored in a table with the database, access to the keys should be limited and under the protection of a secure role with fine grain auditing in place for the table.<br>The column name should be obscure and should not reveal the role of the column.<br>Rows should be protected with both VPD and OLS (OLS included VPD) and the keys themselves should be encrypted with a master key.<br><br>If the keys are managed by an application or generated as computed keys the procedures should be wrapped.<br>All package bodies, procedures, and functions should be wrapped. | Assign multiple layers of protection, within the limits of what can be managed, to ensure the security of the encryption keys. The combination of methods will be dependent on how and where the keys are stored.<br><br>Use multiple layers of protection when storing keys with the data in a separate database.<br><br>Employ wrapping to protect all code used to protect, generate keys for, or encrypt keys.<br><br>If security dictates, hardware devices can be used for encryption key storage.<br><br>Keys, at minimum, should follow password selection standards in areas of minimum length, use of special characters and non-dictionary words. | 10g,9i | √ | √ | 2<br><br>S |
| 5.24 | Encryption | Revoke the PUBLIC execute privileges from the DBMS_OBFUSCATION_TOOL KIT. | The DBMS_OBFUSCATION_TOOLKIT has been replaced with the DBMS_CRYPTO package, but the DBMS_OBFUSCATION_TOOLKIT is still needed for some tasks that are not availabel in the DBMS_CRYPTO package. As an example; the generation of a pseudorandom string requires the DBMS_OBFUSCATION_TOOLKIT. By removing public access to the DBMS_OBFUSCATION_TOOLKIT the means to decrypt the data is not availabel for malicious use. | 10g,9i | √ | √ | 2<br><br>S |

## 6. Startup and Shutdown

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 6.01 | Advanced queuing in asynchronous messaging | Empty queue at shut down of Oracle. | Information in queue may be accessed outside of Oracle and beyond the control of the security parameters. It should be subject to the same security precautions as other tables. | 10g,9i | √ | √ | 1<br>S |
| 6.02 | Cache | Cache must be emptied at shut down of Oracle. | Information in caches may be accessed outside of Oracle and beyond the controls of the security parameters. | 10g,9i | √ | √ | 1<br>S |
| 6.03 | ASM | Ensure that the ASM is started first and shut down last | Ensure that the Automated Storage Management (ASM), new to Oracle 10g, is started first and shut down last. Databases cannot mount their data files until the ASM instance is started, and will crash if the ASM instance is shut down before dependent databases are unmounted. This could cause loss of availability and possible database corruption.<br>Note that this problem is fixed by patching to version 10.1.0.3 or higher. | 10g | √ | √ | 2<br>S |

## 7. Backup and Disaster Recovery

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 7.01 | Redo logs | Mirror | The on-line redo logs must be mirrored and more than one group must exist. | 10g,9i | √ | √ | 1 S |
| 7.02 | Control files | Multiplex control files to multiple physical disks. | Redundancy for the control files can prevent catastrophic loss in the event of a single physical drive failure. | 10g,9i | √ | √ | 1 |
| 7.03 | Control files | Mirror | The control files must be mirrored. | 10g,9i | √ | √ | 1 S |
| 7.04 | Archive logs | Ensure there is sufficient space for the archive logging process. | Without adequate space for the archive logs the system will hang. | 10g,9i | √ | √ | 1 |
| 7.05 | Redo logs | Multiplex redo logs to multiple physical disks. | Redundancy for the redo logs can prevent catastrophic loss in the event of a single physical drive failure. | 10g,9i | √ | √ | 1 |
| 7.06 | Archive log files | Backup | If archivelog mode is used the archive log files must be saved on tape or to a separate disk. File permissions must be restricted to the owner of the Oracle software and the dba group. The archive logs must be secured. | 10g,9i | √ | √ | 1 N |
| 7.07 | Backup | Automated backups should be verified. | Oracle 10g streamlines backups with new automated services. Backups should be verified by performing recoveries to ensure newer automated backups function properly. Failure to ensure this could cause inability to recover data, leading to data loss. The improved RMAN (Recovery Manager) capabilities (i.e., incremental backup process) can be used to facilitate backups and recovery. | 10g | √ | √ | 1 |
| 7.08 | Failsafe | Failsafe must be engaged. | Failsafe uses the cluster server interface to provide the failover protection previously provided by hardware interfaces. | 9i | √ | | 2 |

## 8. Oracle Profile (User) Setup Settings

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 8.01 | Database Profiles | failed_login_attempts=3 | Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database. Application accounts must be set for failed_login_attempts=1.<br>Create a profile then assign it to a user account. Default profile has this setting at 10. | 10g,9i | √ | √ | 1<br>S |
| 8.02 | Database Profiles | password_life_time= 90 | Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.<br>Create a profile then assign it to a user account. Default profile has this setting not set. | 10g,9i | √ | √ | 1<br>S |
| 8.03 | Database Profiles | password_reuse_ max=20 | Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.<br>Create a profile then assign it to a user account. Default profile has this setting not set. | 10g,9i | √ | √ | 1<br>S |
| 8.04 | Database Profiles | password_reuse_ time= 365 | Local policy may not override the setting. This setting must be set to unlimited if a password_reuse_max value other than unlimited is defined for Oracle versions earlier than 9i. See Metalink DocID 228991.1 to see the Oracle version-specific relationship of this setting with the password_reuse_max setting.<br>Create a profile then assign it to a user account. Default profile has this setting not set. | 10g,9i | √ | √ | 1<br>S |
| 8.05 | Database Profiles | password_lock_time=1 | Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.<br>Create a profile then assign it to a user account. Default profile has this set to unlimited. | 10g,9i | √ | √ | 1<br>S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 8.06 | Database Profiles | password_grace_time=3 | Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.<br>Create a profile then assign it to a user account. Default profile has this setting not set. | 10g,9i | √ | √ | 1<br>S |
| 8.07 | Database Profiles | Review accounts where PASSWORD= 'EXTERNAL' | Check and review any user who has password='EXTERNAL'. Do not allow remote OS authentication to the database. | 10g,9i | √ | √ | 2<br>R |
| 8.08 | Database Profiles | Set password_verify_function to a verification function | Allows password verification function to be called when passwords are changed. This always works for password changes via the "password" command at an SQL prompt. It may or may not work with the ALTER USER command. This setting may not be applicable for middle tier application accounts that access the database. Oracle provides utlpwdmg.sql which can be used to create a password verification function. If using this script to create a password verification function, make the following changes at the bottom of the utlpwdmg.sql file:<br>PASSWORD_GRACE_TIME 3<br>PASSWORD_REUSE_TIME 365<br>PASSWORD_REUSE_MAX 20<br>FAILED_LOGIN_ATTEMPTS 3<br>PASSWORD_LOCK_TIME 1<br>Modify the line: IF length(password) < 4<br>by changing the minimum password length to 8. | 10g,9i | √ | √ | 2<br>S |
| 8.09 | Database Profiles | Set CPU_PER_ SESSION as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. | 10g,9i | √ | √ | 2<br>R |
| 8.10 | Database Profiles | Set PRIVATE_SGA as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. This only applies when shared/multi-threaded server is in use. | 10g,9i | √ | √ | 2<br>R |
| 8.11 | Database Profiles | Set LOGICAL_READS_ PER_SESSION as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. | 10g,9i | √ | √ | 2<br>R |
| 8.12 | Database Profiles | Set SESSIONS_PER_ USER as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. | 10g,9i | √ | √ | 2<br>R |
| 8.13 | Database Profiles | Set CONNECT_TIME as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. | 10g,9i | √ | √ | 2<br>R |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 8.14 | Database Profiles | Set IDLE_TIME as appropriate | Ensure that users profile settings have appropriate values set for the particular database and application. | 10g,9i | √ | √ | 2 R |

## 9. Oracle Profile (User) Access Settings

**Note:** Security recommendations for Tablespaces, Tables, Views, Roles, Synonyms, Privileges, Roles and Packages need to be followed for all new users that might be created. By default sys has most of these accesses and privileges, and should be the only user with them.

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 9.01 | Tablespaces | Do not have default_tablespace set to SYSTEM for user accounts | Only SYS should have a default tablespace of SYSTEM. It may be difficult or impossible to move some objects. | 10g,9i | √ | √ | 1 S |
| 9.02 | Tablespaces | Ensure application users have not been granted quotas on tablespaces. | Set quotas for developers on shared production/development systems to prevent space resource contentions. | 10g,9i | √ | √ | 1 S |
| 9.03 | Any dictionary object | Review access and revoke access as possible | Check for any user that has access to any dictionary object and revoke where possible. | 10g,9i | √ | √ | 1 R |
| 9.04 | Tables | Prevent access to SYS.AUD$ | Check for any user other than SYS and DBA accounts that have access and revoke where possible. This is only applicable if the audit trail parameter is set to DB or TRUE. | 10g,9i | √ | √ | 1 S |
| 9.05 | Tables | Prevent access to SYS.USER_ HISTORY$ | Revoke access to this table from all users and roles except for SYS and DBA accounts. | 10g,9i | √ | √ | 1 S |
| 9.06 | Tables | Prevent access to SYS.LINK$ | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.07 | Tables | Prevent access to SYS.USER$ | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.08 | Tables | Prevent access to SYS.SOURCE$ | Check for any user other than SYS and DBA accounts that have access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.09 | Tables | Prevent access to PERFSTAT.STATS$SQLTEXT | Check for any user that has access and revoke where possible | 10g,9i | √ | √ | 1 S |
| 9.10 | Tables | Prevent access to PERFSTAT.STATS$SQL_SUM MARY | Check for any user that has access and revoke where possible | 10g,9i | √ | √ | 1 S |
| 9.11 | Tables | Prevent access to any X$ table | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.12 | Views | Prevent access to any DBA_ views | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 9.13 | Views | Prevent access to any V_$ views | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.14 | Views | Prevent access to ALL_SOURCE | Check for any user other than SYS that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.15 | Views | Prevent access to DBA_ROLES | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.16 | Views | Prevent access to DBA_SYS_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.17 | Views | Prevent access to DBA_ROLE_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.18 | Views | Prevent access to DBA_TAB_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.19 | Views | Prevent access to DBA_USERS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.20 | Views | Prevent access to ROLE_ROLE_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.21 | Views | Prevent access to USER_TAB_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.22 | Views | Prevent access to USER_ROLE_PRIVS | Restrict access to this view to all users except SYS and DBAs. | 10g,9i | √ | √ | 1 S |
| 9.23 | Roles | Prevent assignment of roles that have _CATALOG_ | Revoke any catalog roles from those roles and users that do not need them. These roles are SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE, DELETE_CATALOG_ROLE, and RECOVERY_CATALOG_OWNER. | 10g,9i | √ | √ | 1 R |
| 9.24 | Synonyms | Prevent access to any V$ synonym | Check for any user that has access and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.25 | Synonyms | When dropping synonyms, ensure privileges granted to the synonyms, if not required, are removed from the base objects. | Granting privileges to synonyms actually grants privileges to the base objects. If necessary, ensure that privileges from the base objects are removed when the synonyms are dropped. | 10g,9i | √ | √ | 1 |
| 9.26 | Privileges | Restrict system privileges | All system privileges except for CREATE SESSION must be restricted to DBAs, application object owner accounts/schemas (locked accounts) and default Oracle accounts. Developers may be granted limited system privileges as required on development databases. | 10g,9i | √ | √ | 1 S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 9.27 | Privileges | Prevent granting of privileges that contain the keyword ANY | Check for any user or role that has the “ANY” keyword and revoke this role where possible. | 10g,9i | √ | √ | 1 S |
| 9.28 | Privileges | Prevent granting of ALL PRIVILEGES | The GRANT ALL PRIVILEGES must not be used. | 10g,9i | √ | √ | 1 N |
| 9.29 | Privileges | Prevent granting of EXEMPT ACCESS POLICY (EAP) | Revoke this privilege if not necessary. The EAP privilege provides access to all rows regardless of Row Level Security assigned to specific rows. | 10g,9i | √ | √ | 1 S |
| 9.30 | Privileges | Prevent granting of privileges that have WITH ADMIN | Check for any user or role that has been granted privileges “with admin” and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.31 | Privileges | Prevent granting of privileges that have WITH GRANT | Check for any user or role that has been granted privileges “with grant” and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.32 | Privileges | Prevent granting of privileges that have CREATE | Check for any user that has object creation privileges and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.33 | Privileges | Prevent granting of CREATE LIBRARY | Check for any user or role that has this privilege and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.34 | Privileges | Prevent granting of ALTER SYSTEM | Check for any user or role that has this privilege and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.35 | Privileges | Prevent granting of CREATE PROCEDURE | Check for any user or role that has this privilege and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.36 | Privileges | Prevent granting of BECOME USER | Check for any user or role that has this privilege and revoke where possible. | 10g,9i | √ | √ | 1 S |
| 9.37 | Privileges | Prevent granting of SELECT ANY TABLE | Check for any user that has access and revoke where possible. If application data is sensitive, and it is possible, revoke this privilege from the DBA accounts as well. | 10g,9i | √ | √ | 1 S |
| 9.38 | Privileges | Prevent granting of AUDIT SYSTEM | Review which users have audit system privileges and limit as much as possible to ensure audit commands are not revoked. | 10g,9i | √ | √ | 1 S |
| 9.39 | Privileges | Grant privileges only to roles. | Grant privileges only to roles. Do not grant privileges to individual users. | 10g,9i | √ | √ | 1 S |
| 9.40 | Privileges | Review privileges granted to PUBLIC | Review all privileges granted to PUBLIC. Limit or revoke unnecessary PUBLIC privileges. | 10g,9i | √ | √ | 1 R |
| 9.41 | Roles | Prevent assignment of RESOURCE | Revoke the resource role from normal application user accounts. | 10g,9i | √ | √ | 1 S |
| 9.42 | Roles | Prevent assignment of CONNECT | Revoke connect role from normal application user accounts. | 10g,9i | √ | √ | 1 S |
| 9.43 | Roles | Prevent assignment of DBA | Revoke dba role from users who do not require it. | 10g,9i | √ | √ | 1 R |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 9.44 | Packages | Deny access to UTL_FILE | Revoke the public execute privilege on utl_file as it can be used to access O/S<br>Only sys has privilege by default. | 10g,9i | √ | √ | 1<br>S |
| 9.45 | Packages | Deny access to UTL_TCP | Revoke the public execute privilege on utl_tcp as it can write and read sockets.<br>Only sys has privilege by default. | 10g,9i | √ | √ | 1<br>S |
| 9.46 | Packages | Deny access to UTL_HTTP | Revoke the public execute privilege on utl_http as it can write content to a web browser.<br>Only sys has privilege by default. | 10g,9i | √ | √ | 1<br>S |
| 9.47 | Packages | Deny access to UTL_SMTP | Revoke the public execute privilege on utl_smtp as it can send mail from the database server.<br>Only sys has privilege by default. | 10g,9i | √ | √ | 1<br>S |
| 9.48 | Packages | Deny access to DBMS_LOB | Revoke the public execute privilege. | 10g,9i | √ | √ | 1 S |
| 9.49 | Packages | Deny access to DBMS_SYS_SQL | Revoke the public execute privilege. | 10g,9i | √ | √ | 1<br>S |
| 9.50 | Packages | Deny access to DBMS_JOB | Revoke the public execute privilege. | 10g,9i | √ | √ | 1 S |
| 9.51 | Proxy Authentication | Limit the user schema privileges to “CREATE SESSION” only. | The proxy account should only have the ability to connect to the database. No other privileges should be granted to this account.<br>Set when creating the proxy account. | 10g,9i | √ | √ | 1 |
| 9.52 | Proxy role | Restrict the roles that can be enabled when privileges are granted in the database. As an example;<br><br>“CREATE ROLE ‘X” “<br>“GRANT ‘X’ TO JOHN_SMITH”<br>“ALTER USER JOHN_SMITH DEFAULT ROLE ALL EXCEPT X” | Assuming John Smith needs only the role of ‘X’, then all other roles are prevented from being enabled. | 10g,9i | √ | √ | 1 |
| 9.53 | Tables | Do not store passwords in clear text in Oracle tables | Passwords stored by applications in the database tables must be encrypted. Access to these tables must be limited. | 10g,9i | √ | √ | 2<br>N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 9.54 | Tables | Encrypt critical data | Critical data must be encrypted to prevent the DBA from accessing it. Alternately, audit key tables. This does not prevent the DBA from viewing the data, but would create a record of the activity. Management of the encryption key must be done carefully as exposure of the key will render the encryption moot. | 10g,9i | √ | √ | 2<br><br>N |
| 9.55 | Views | Revoke public access to all public views that start with ALL_ | Revoke access to these views when possible. This may interfere with some applications. | 10g,9i | √ | √ | 2<br>S |
| 9.56 | Roles | Password protect roles | Role passwords are useful when an application controls whether or not a role is turned on. This prevents a user directly accessing the database via SQL (rather than through the application) from being able to enable the privileges associated with the role. | 10g,9i | √ | √ | 2<br><br>S |
| 9.57 | Roles and Privileges | When dropping a user, ensure roles and privileges created by that user, if not required, are deleted. | If a user is dropped, ensure that the roles and privileges created by that user, if not required, are deleted. Dropping a user (i.e., DROP USER X CASCADE) doesn't delete roles and privileges created by the user. | 10g,9i | √ | √ | 2 |
| 9.58 | Packages | Limit or deny access to dbms_backup_restore | Provides file system functions such as copying files, altering control files, accessing devices, and deleting files. | 10g,9i | √ | √ | 2<br><br>S |
| 9.59 | Packages | Limit or deny access to DBMS_RANDOM | Revoke the public execute privilege. | 10g,9i | √ | √ | 2<br>S |

## 10. Enterprise Manager / Grid Control / Agents

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 10.01 | Enterprise Management studio mode | Access to the enterprise management in studio must be limited. | Without limitations on the enterprise management access to the remote agents is virtually unlimited. | 10g,9i | √ | √ | 1 |
| 10.02 | Enterprise Manager Agent File uploads | Monitor the size of file uploads from the enterprise agent. | The following lines are some of the output from the ./emctl status agent command containing information regarding the agents uploading files:<br><br>Total Megabytes of XML files uploaded so far : Number of XML files pending upload:<br>Size of XML files pending upload(MB):<br><br>Discovering unusual or increased size of file uploads could indicate a malicious agent. | 10g | √ | √ | 1 |
| 10.03 | Enterprise Manager Framework Security | Where possible, utilize Enterprise Manager Framework Security Functionality. | Enterprise Manager Framework security employs secure communication between the various Enterprise Manager Components, i.e., HTTPS between management agents and management services. | 10g | √ | √ | 1 |
| 10.04 | Grid Control TimeOut Value | Configure an appropriate value for Grid Control Timeout value in the Oracle Application Server.<br>File:<br>IAS_HOME/sysman/config/emoms.properties<br><br>Value:<br>oracle.sysman.eml.maxInactiveTime=time_in_minutes | To prevent unauthorized access to the Grid Control via browser, set an appropriate timeout value.<br>The default is 45 minutes. | 10g | √ | √ | 1 |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 10.05 | Enterprise Manager Framework Security | In command line mode, avoid using commands that contain passwords in the arguments. | While registering an agent to utilize the enterprise manager framework security, avoid using the complete command line arguments for the emctl command.<br><br>The command can be captured by other users with access to unix (via ps) command or can be prone to shoulder surfing. | 10g | √ | √ | 1 |
| 10.06 | Oracle Installation | Separate user account for Management/Intelligent Agent | For Unix systems, create a unique user account for the management/Intelligent Agent process in order to differentiate accountability and file access controls. The agent database accounts must be separated. Separate accounts are not recommended for Windows environments. | 10g,9i | | √ | 2 |

## 11. 10g Specific Systems

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 11.01 | ADDM | Verify ADDM suggestions | Oracle 10g's new automated diagnostics through the Automatic Database Diagnostic Monitor (ADDM), should not blindly replace the DBA's knowledge. DBA's should verify the applicability of ADDM suggestions based on their knowledge of the database. | 10g | √ | √ | 1 |
| 11.02 | AMM | Monitor AMM | Oracle 10g's new Automated Memory Manager (AMM), should not blindly replace the DBA's knowledge. DBA's should monitor AMM to ensure memory is being properly allocated. | 10g | √ | √ | 1 |
| 11.03 | AWR | Implement AWR to record all database performance statistics (related to object usage, SQL statement efficiency, session history, etc) over a defined time period. | Automatic Workload repository (AWR) is central to the whole framework of self and automatic management. It works with internal Oracle database components to process, maintain, and access performance statistics for problem detection and self-tuning. The statistics are availabel to external users or performance monitoring tools, routines, or scripts. Trends analysis can be done with AWR data. Queries that overtax the system could be a security threat. | 10g | √ | √ | 1 |
| 11.04 | Fine grained access | Use fine grain access control within objects. | Fine grained access control can provide both column and row level security. This can provide an additional layer of access control to objects by limiting the access (select, update, insert, delete) within the object and should be used wherever possible. For fine grained access to function properly, use the cost-based optimizer. | 10g | √ | √ | 2 |

## 12. General Policy and Procedures

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.01 | Oracle alert log file | Review contents | The Oracle alert log file must be regularly reviewed for errors. | 10g,9i | √ | √ | 1 N |
| 12.02 | Database creation scripts on host | Remove or secure | After the database has been created, remove the scripts or at a minimum move them to a safe repository area. | 10g,9i | √ | √ | 1 S |
| 12.03 | Unix root group members on host | Disallow 'oracle' as member of root group | The Oracle software owner account must not be a member of the root group on Unix systems. | 10g,9i | | √ | 1 |
| 12.04 | Oracle DBA group membership on host | Review | Review the membership of the DBA group on the host to ensure that only authorized accounts are included. This must be limited to users who require DBA access. | 10g,9i | √ | √ | 1 R |
| 12.05 | Sensitive information in process list on host | Avoid or encrypt | An enforced policy must exist to ensure that no scripts are running that display sensitive information in the process list such as the Oracle username and password. A privileged process must be used to get and decrypt encrypted passwords. | 10g,9i | √ | √ | 1 N |
| 12.06 | Sensitive information in cron jobs on host | Avoid or encrypt | An enforced policy must exist to ensure that no cron jobs have sensitive information such as database username and passwords. A privileged process must be used to get and decrypt encrypted passwords. | 10g,9i | | √ | 1 |
| 12.07 | Sensitive information in at jobs (or jobs in Windows scheduler) on host | Avoid or encrypt | An enforced policy must exist to ensure that no at jobs (or jobs in Windows scheduler) has sensitive information such as database username and passwords. A privileged process must be used to get and decrypt encrypted passwords. | 10g,9i | √ | √ | 1 |
| 12.08 | Sensitive information in environment variables on host | Avoid or encrypt | An enforced policy must exist to ensure that no users have unencrypted sensitive information such as database username and passwords set in environment variables. A privileged process must be used to get and decrypt encrypted passwords. | 10g,9i | √ | √ | 1 N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.09 | Sensitive information in batch files on host | Avoid or encrypt | An enforced policy must exist to ensure that no batch files have unencrypted sensitive information such as database username and passwords. A privileged process must be used to get and decrypt encrypted passwords. | 10g,9i | √ | √ | 1<br>N |
| 12.10 | Oracle file locations | Separate for performance | Split the location of the Oracle software distribution, redo logs, data files, and indexes onto separate disks and controllers for resilience. | 10g,9i | √ | √ | 1<br>Y |
| 12.11 | File systems | Separate Oracle files from non-Oracle files | Only put database files on file systems exclusively used by Oracle. Oracle files must not be on the same partition as the operating system. | 10g,9i | √ | √ | 1<br>Y |
| 12.12 | Optimal Flexible Architecture | Implement | Follow the Oracle Optimal Flexible Architecture guidelines to provide for consistency and ease of administration. | 10g,9i | √ | √ | 1<br>N |
| 12.13 | Checksum PL/SQL code | Implement | Store the checksum results and periodically check for alterations. | 10g,9i | √ | √ | 1<br>N |
| 12.14 | All database objects | Monitor | Store the results of the time stamps of the creation, reload, and compilation of database objects and review the results regularly to ensure no unauthorized changes have occurred. | 10g,9i | √ | √ | 1<br>N |
| 12.15 | Ad-hoc queries on production databases | Avoid | Disallow ad-hoc queries on production databases. This recommendation may not be suitable for all environments, for example, data warehouses. | 10g,9i | √ | √ | 1<br>N |
| 12.16 | Media integrity | Verify | Backup media integrity must be checked regularly. | 10g,9i | √ | √ | 1 N |
| 12.17 | Remote shell access on host | Encrypt session | If remote shell access is required, use ssh or a VPN solution to ensure that session traffic is encrypted. In a cluster environment (RAC or OPS) rsh and rcp are required between the nodes for the Oracle software owner. In the case of a cluster environment, the access must be restricted by user and host. | 10g,9i | √ | √ | 1<br>N |
| 12.18 | Applications with database access | Review | Review and control which applications access the database. | 10g,9i | √ | √ | 1<br>N |
| 12.19 | Location of development database | Separate server from production database | Test and development databases must not be located on the same server as the production system. | 10g,9i | √ | √ | 1<br>N |
| 12.20 | Network location of production and development databases | Separate | If possible, place production databases on a different network segment from test and development databases. | 10g,9i | √ | √ | 1<br>N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.21 | Monitor for development on production databases | Prevent development on production databases | Check for evidence of development occurring on production databases. | 10g,9i | √ | √ | 1<br>N |
| 12.22 | Access to production databases | Avoid access from development or test databases | Database access from development and test databases to production databases must be prohibited. | 10g,9i | √ | √ | 1<br>N |
| 12.23 | Developer access to production databases | Disallow | Developers must not have direct access to production databases. | 10g,9i | √ | √ | 1<br>N |
| 12.24 | Developer accounts on production databases | Remove | Remove any developer accounts that exist in the production database. | 10g,9i | √ | √ | 1<br>N |
| 12.25 | Databases created from production exports | Change passwords | If test or development databases are created from backups or exports of the production system, all passwords must be changed before granting access to developers or testers. | 10g,9i | √ | √ | 1<br>N |
| 12.26 | Databases created from production systems | Remove sensitive data | If test or development databases are created from backups or exports of the production system, all sensitive data (such as payroll information) must be removed before granting access to developers or testers. | 10g,9i | √ | √ | 1<br>N |
| 12.27 | Account Management | Document and enforce account management procedures | Create and regularly review procedures for account management. This must include the creation of new user accounts, moving a user to a new group or role, and handling of dormant or inactive accounts. | 10g,9i | √ | √ | 1<br>N |
| 12.28 | Change Control | Document and enforce change control procedures | Create and regularly review procedures for new applications that access the database and change control management procedures for releasing development code into production. Monitor the addition of new users and access rights. | 10g,9i | √ | √ | 1<br>N |
| 12.29 | Disaster recovery procedures | Review | Disaster recovery procedures must be fully documented and regularly tested. | 10g,9i | √ | √ | 1<br>N |
| 12.30 | Backdoors | Eliminate | Tight change control management procedures and checksums of the source code can help prevent backdoors into the database. | 10g,9i | √ | √ | 1<br>N |
| 12.31 | Public dissemination of database information | Disallow | The posting database information such as SIDs, hostnames, and IP addresses to newsgroups and mailing lists must not be allowed. | 10g,9i | √ | √ | 1<br>N |
| 12.32 | Screen saver | Set screen saver/lock with password protection of 15 minutes. | If an organizational policy does not exist, 15 minutes must be set as the standard. | 10g,9i | √ | √ | 1<br>N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.33 | Distribution of tnsnames.ora files to clients | Include only necessary tnsnames.ora when distributing to clients | If clients connect to the database using tnsnames.ora files, ensure that only necessary entries are included in the file when distributing to clients. | 10g,9i | √ | √ | 1<br>N |
| 12.34 | Put database in archivelog mode (if appropriate to database function). | If the database was not created in archivelog mode, start the database in mount mode, and issue: alter database achivelog; | If archive log mode is used, transmission of archive logs must be secured as LogMiner could be used to extract database information from the archive logs. | 10g,9i | √ | √ | 1<br>S |
| 12.35 | Event and System Logs | Monitor | Windows Event Logs and Unix System logs must be regularly monitored for errors related to the Oracle database. | 10g,9i | √ | √ | 1 |
| 12.36 | Access to database objects by a fixed user link | Disallow | Fixed user database links that have a hard coded username and password must be avoided. | 10g,9i | √ | √ | 1<br>S |
| 12.37 | Oracle Installation | Oracle software owner account name NOT 'oracle' | Do not name the Oracle software owner account 'oracle' as it is very well known. | 10g,9i | √ | √ | 2<br>S |
| 12.38 | Oracle Installation | Separate users for different components of Oracle | For Unix systems, create unique user accounts for each Oracle process/service in order to differentiate accountability and file access controls. The listener, the Oracle http server, and the database process accounts must be separate. Separate accounts are not recommended for Windows environments. The requirement for the Management/Intelligent Agent process is listed in section 10 of this document. | 10g,9i | | √ | 2 |
| 12.39 | Alerts on high priority incidents | Create processes to alert | Create processes to monitor and alert of high priority incidents. | 10g,9i | √ | √ | 2<br>N |
| 12.40 | Intelligent agent | Do not use | If the database server is accessible via the Internet, do not use the Intelligent Agent. This may not be practical for OEM or SNMP monitored databases. | 10g,9i | √ | √ | 2<br>S |
| 12.41 | Oracle Advanced Security | Implement if appropriate | If appropriate to the environment, implement Oracle Advanced Security to encrypt all traffic between the client and server. | 10g,9i | √ | √ | 2<br>S |
| 12.42 | Application PL/SQL code | Wrap | The wrap program provided by Oracle encodes the PL/SQL source code but does not encrypt it. | 10g,9i | √ | √ | 2<br>S |
| 12.43 | PL/SQL code variables and constants | Obscure | The wrap program does not encode variables and constants. | 10g,9i | √ | √ | 2<br>N |
| 12.44 | Hard coded data in PL/SQL code | Avoid or encrypt | Do not use unencrypted hard coded usernames, passwords, or other critical data in the PL/SQL code. | 10g,9i | √ | √ | 2<br>N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.45 | Decommissioned applications | Remove all components | Ensure that all associated binaries, users, batch process, and access rights are removed when applications are decommissioned. | 10g,9i | √ | √ | 2 N |
| 12.46 | Usernames and passwords | Do not hardcode in application source code | Do not hard code usernames and passwords in application source code. Set username and passwords in an encrypted external file or database table. | 10g,9i | √ | √ | 2 N |
| 12.47 | DDL statements in application | Disallow | Applications must not alter the database schema. | 10g,9i | √ | √ | 2 N |
| 12.48 | Reporting tool interface and authentication | Review | Any remote access to the database host must be controlled by an application level firewall. | 10g,9i | √ | √ | 2 N |
| 12.49 | Enabling of batch process account | Time enabled | The account that is used to run batch processes must be enabled only during the time that the batch processes run. | 10g,9i | √ | √ | 2 N |
| 12.50 | Passwords for batch processes | Secure | Passwords for batch processes must not be a command line parameter or an environment variable. | 10g,9i | √ | √ | 2 N |
| 12.51 | External account access for batch processes | Disallow | External accounts used for batch processes allow a simple way to access the database. | 10g,9i | √ | √ | 2 N |
| 12.52 | Object and table owners | Review | Identify the owner of all objects and tables that make up an application. | 10g,9i | √ | √ | 2 R |
| 12.53 | Data in development database | Protect | If data is imported from a production database to development or test databases, ensure that any sensitive data (i.e. payroll information) is not accessible to users of the development or test databases. | 10g,9i | √ | √ | 2 N |
| 12.54 | Database links to production databases | Avoid links from development database | Database links from development and test databases to production databases must be forbidden. | 10g,9i | √ | √ | 2 N |
| 12.55 | User permissions | Review | Review and test development databases for users with excess permissions not granted in production. | 10g,9i | √ | √ | 2 N |
| 12.56 | Procedures for backup tape retrieval | Review | Ensure the procedures for backup tape retrieval are documented and are adequate to prevent social engineering attacks to steal data. | 10g,9i | √ | √ | 2 N |
| 12.57 | Intrusion detection system on host | Utilize | Use a host based Intrusion Detection System on the server hosting the Oracle database. | 10g,9i | √ | √ | 2 N |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 12.58 | Multiple listeners | Create separate listeners for clients and administration. Protect the administrative listener with IPSec ESP or OAS SSL and a personal firewall. | An administrative listener, protected by IPSec, could allow administrators access to the server if the client listener(s) are taken down. Preference of implementation is IPSec ESP, otherwise SSL and personal firewall. If SSL is not possible, use OAS native encryption/integrity with a personal firewall, otherwise use a personal firewall. Access must be limited to specific administrative workstations. | 10g,9i | √ | √ | 2<br>N |
| 12.59 | Remote Administration of Listener | Configure listener to have an SSL port. | If remote administration of a listener via the listener utility is required, e.g., no administration through SSH or MS Terminal Server, configure the listener to have a TCPS (SSL) port. If the listener is configured to use multiple protocols, set the SSL protocol as the first protocol in listener.ora. | 10g,9i | √ | √ | 2<br>N |
| 12.60 | Policy Caching | Policy caches must be purged. | Policy caches can potentially store information that could be used to compromise the database and may accessible outside of Oracle and beyond the control of the security parameters. Hence this can defeat row level security. | 10g,9i | √ | √ | 2 |
| 12.61 | Policy Functions | Users should not have execute, alter or drop privileges on policy functions. | The ability to manipulate policy functions could be used to defeat row level security. | 10g,9i | √ | √ | 2 |
| 12.62 | Passwords | Remove password parameters from configuration files utilized for Silent Installations. | Whenever utilizing silent installs, i.e., Oracle Installer, ensure configuration files do not contain password values after the installation completes. | 10g,9i | √ | √ | 2 |
| 12.63 | Security of transmitted data | Any data sent over a network must be secure or must be sent via a secure protocol. | Data sent over a network can reveal significant information. Any data should be secure. If the network structure itself is not secure, data must be sent via a secure protocol. | 10g | √ | √ | 2 |

## 13. Auditing Policy and Procedures

**Note:** By default all auditing is turned off except auditing of the sys account. Fine Grain auditing is off by default.

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 13.01 | Auditing | Unused schemas should be dropped | Unused schemas should be first audited to ensure that they are in fact unused. After verification, they should be dropped. | 10g,9i | √ | √ | 2 |
| 13.02 | Auditing | Trap autonomous transactions | This will ensure that audit captures actions performed by users even if they are later rolled back. | 10g,9i | √ | √ | 2 |
| 13.03 | Auditing | Audit all log ons and log offs. | This is the minimum of auditing and the auditing must be configured to show who logged on/off. | 10g,9i | √ | √ | 2 |
| 13.04 | Auditing | Audit for unsuccessful attempts. Audit by "ACCESS WHENEVER NOT SUCCESSFUL". | Auditing by SESSION will only show a single audit event for an attempt. By logging unsuccessful attempts any SQL statement attempting to access the table will be recorded. This could provide a record of unauthorized attempts to access sensitive data. | 10g,9i | √ | √ | 2 |
| 13.05 | Auditing | Where appropriate or required by security or legal requirements, engage and use the Fine-Grained Auditing feature. | Because the FGA record entry can be pre-qualified, it should not add a significant burden to the size of audit records. The flexibility, column specific sensitivity, capture of the SQL, and the event handler combine to make it a valuable asset. | 10g,9i | √ | √ | 2 |
| 13.06 | Auditing | Where appropriate or required by security or legal requirements, use enhanced capabilities of Fine-Grained Auditing. | Fine Grain Auditing (FGA) in Oracle 10g can now audit all types of Data Manipulation Language (DML) statements, not just SELECT. Consider using this to enhance current auditing capabilities. FGA can also optionally execute procedures. For instance, a procedure could perform an action such as sending an e-mail alert to an auditor when a user selects a certain row from a table, or it could write to a different audit trail. | 10g | √ | √ | 2 |
| 13.07 | Auditing | Audit ALTER ANY TABLE | Audit the use of ALTER ANY TABLE. | 10g,9i | √ | √ | 2 S |
| 13.08 | Auditing | Audit ALTER USER | Audit the use of ALTER USER. | 10g,9i | √ | √ | 2 S |
| 13.09 | Auditing | Audit any CREATE statement | Audit the use of any CREATE statement. | 10g,9i | √ | √ | 2 S |
| 13.10 | Auditing | Audit CREATE ROLE | Audit the use of CREATE ROLE. | 10g,9i | √ | √ | 2 S |
| 13.11 | Auditing | Audit CREATE USER | Audit the use of CREATE USER. | 10g,9i | √ | √ | 2 S |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 13.12 | Auditing | Audit CREATE SESSION | Audit the use of CREATE SESSION for successful or unsuccessful operations. | 10g,9i | √ | √ | 2 S |
| 13.13 | Auditing | Audit any DROP statement | Audit the use of any DROP statement. | 10g,9i | √ | √ | 2 S |
| 13.14 | Auditing | Audit DROP ANY PROCEDURE | Audit the use of DROP ANY PROCEDURE. | 10g,9i | √ | √ | 2 S |
| 13.15 | Auditing | Audit DROP ANY TABLE | Audit the use of DROP ANY TABLE. | 10g,9i | √ | √ | 2 S |
| 13.16 | Auditing | Audit GRANT ANY PRIVILEGE | Audit the use of GRANT ANY PRIVILEGE. | 10g,9i | √ | √ | 2 S |
| 13.17 | Auditing | Audit GRANT ANY ROLE | Audit the use of GRANT ANY ROLE. | 10g,9i | √ | √ | 2 S |
| 13.18 | Auditing | Audit INSERT failures | Audit INSERT failures attempted into critical data objects. | 10g,9i | √ | √ | 2 S |
| 13.19 | Auditing | Logon, logoff, database start or stop, and other information. | Create triggers against all tables and system events that are meaningful to the database and application. | 10g,9i | √ | √ | 2 N |
| 13.20 | Auditing | Use triggers to implement row level auditing | Use triggers to enforce row level auditing for important data. | 10g,9i | √ | √ | 2 N |
| 13.21 | Auditing | Review procedures and reports to review audit logs | Regular, timely reviews of the collected audit information must be done. | 10g,9i | √ | √ | 2 N |
| 13.22 | Auditing | Set AUDIT ALL ON SYS.AUD$ BY ACCESS | By setting AUDIT ALL ON SYS.AUD$ BY ACCESS, attempts to alter the audit trail will be audited. Only applicable if the audit trail parameter is set to DB or TRUE. | 10g,9i | √ | √ | 2 S |
| 13.23 | Auditing | Regularly purge the audit trail | Review the purging procedures to ensure that the audit trail is purged regularly. | 10g,9i | √ | √ | 2 N |

## Appendix A – Additional Settings (not scored)

**Note:** The default 10g database installation does not install Oracle label Security (OLS). OLS must be installed by selecting a custom installation and manually selecting it.

Oracle Advanced Security (OAS) is installed with Oracle 10g. It is available for 9i as well, but as an extra charge. For 9i, OAS items are not scored and are considered additional settings, please see section 3 for those settings.

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version<br><br>10g / 9i | Windows | Unix | Level<br><br>If known |
|---|---|---|---|---|---|---|---|
| 14.01 | Oracle Label Security | Where possible use Oracle Label Security. | OLS is a strong additional layer of security (and can be implemented without significant Oracle experience.) Do we really want to say this? I would suggest:<br><br>OLS is a strong additional layer of security that can be used to create a Virtual Private database (VPD). OLS allows data of varying sensitivities to be stored in a single database and access to the data to be restricted using security clearances as defined by role level. | 10g,9i | √ | √ | 2 |
| 14.02 | Oracle Label Security | Where possible, when using OLS, hide the label column. This can be done by passing the "HIDE" directive to the "DEFAULT_OPTIONS" parameter of the "SA_SYSDBA.CREATE_POLICY" (globally) or to the "TABLE_OPTIONS" parameter of the "APPLY_TABLE_POLICY" proceedure (for a specific table).<br><br>Note: After applying a OLS policy to a table, the hidden status of the labels cannot be revoked without the loss of the labels. | If the status of the hidden label column needs to be changed, the values of the label column may be copied to an added column, then the hidden column can be removed, the column copied, then remove the policy dropping the row label column. Reinstate the policy and then copy the values from the added column to the row label column and then remove the added column. | 10g,9i | √ | √ | 2 |

| Item # | Configuration Item | Action / Recommended Parameters | Comments | Version 10g / 9i | Windows | Unix | Level If known |
|---|---|---|---|---|---|---|---|
| 14.03 | Oracle Label Security | Include the LABEL_UPDATE as a value for table_options parameter when the OLS policy is applied to a table. | This ensures the user cannot reclassify the data in the record by changing the label. | 10g,9i | √ | √ | 2 |
| 14.04 | Oracle Label Security | Where possible, use a trusted procedure to limit and control the manipulation of the labels. | By the creation of a procedure, direct manipulation by database users of the labels is prevented and an additional level of security is provided. This can provide a separation of responsibility between the DBA and the security administrators. | 10g,9i | √ | √ | 2 |
| 14.05 | Oracle Label Security | Have a secure and separate data copy before implementing OLS. | OLS introduces an additional hidden column into a table. For some tables the addition of a column or a hidden column may render the table unusable. For applications that expect to see all the data, OLS may be interpreted as corrupt data. | 10g,9i | √ | √ | 2 |
| 14.06 | Oracle Label Security | Where applicable and possible, store labels in the Oracle Internet Directory (OID). | In the context of Enterprise User Security option this provides a centralized management method for user passwords, enterprise roles, and OLS authorization. Under the control of the OID, policies cannot be manipulated within the databases. | 10g,9i | √ | √ | 2 |
| 14.07 | RAID file systems | Implement | File systems holding the Oracle data should be on RAID volumes for resilience. | 10g,9i | √ | √ | 2 |
| 14.08 | Magnetically wipe failed disks | Implement | Magnetically wipe old, no longer used, or failed disks. This issue is most likely handled by system administrators. | 10g,9i | √ | √ | 2 |
| 14.09 | Backups on system disks | Verify permissions | In many environments, database backups are written to system disks. In this type of environment, ensure that the backup files are protected. Files should be owned by oracle software owner set with owner read/write permissions only. | 10g,9i | √ | √ | 2 |
| 14.10 | Off site backup storage | Implement | Implement off site backup storage procedures. | 10g,9i | √ | √ | 2 |
| 14.11 | Recovery procedures | Document and Test | Ensure that database recovery procedures are fully documented and regularly tested. | 10g,9i | √ | √ | 2 |
| 14.12 | Backup and restore procedures | Document and Test | Ensure that database backup and restore procedures are fully documented and regularly tested. | 10g,9i | √ | √ | 2 |
| 14.13 | Screening router | Implement to restrict access to database host | Implement a screening router to restrict access to the database host. | 10g,9i | √ | √ | 2 |
| 14.14 | Personal fiirewall | Implement on database administration machines | Use a personal firewall on all computers used to administer databases. | 10g,9i | √ | √ | 2 |

**Appendix B – Disabled Windows 2000 Services**

This appendix contains a list of services that, if not needed should be disabled on a Windows 2000 server running Oracle. This is intended as a guide to be used in disabling Windows services.

| Windows 2000 Service |
|---|
| Alerter |
| ClipBook Server |
| Computer Browser |
| DHCP Client |
| Distributed File System |
| Fax Service |
| Internet Connection Sharing |
| IPSEC Policy Agent (Disable unless IPSEC policies will be used.) |
| License Logging Service |
| Logical Disk Manager Administrative Service |
| Messenger |
| NetMeeting Remote Desktop Sharing |
| Network DDE |
| Network DDE DSDM |
| OracleOraHome90HTTPServer (Disable unless iSQL or other web resource is required.) Note: may have a different name. |
| Print Spooler |
| Remote Access Auto Connection Manager |
| Remote Access Connection Manager |
| Remote Registry Service (Disable unless running hfnetchk or similar utilities.) |
| Removable Storage |
| RunAs Service |
| Smart Card |
| Smart Card Helper |
| Telephony |
| Telnet |
| Windows Installer |
| Workstation (Disable unless the server will be part of a domain.) |

**Appendix C – FIPS140-2 Issues**

User communities implementing an Oracle 10g database that are required to meet the FIPS140-2 standard of encryption are facing a unique problem. To set the Oracle 10g software to the FIPS140 standard requires the SQLNET.FIPS_140 setting be set to TRUE and in turn the SQLNET.ENCRYPTION_TYPES_SERVER setting be set to DES|DES40. With the SQLNET_140 set to TRUE any setting other than DES|DES40 for the SQLNET.ENCRYPTION_TYPES_SERVER may cause an error, but the DES or DES40 standard for encryption are at best weak standards and are already subject to several known compromises. See notes 5.02 and 5.03.

Even as DES is an accepted standard for legacy systems under current FIPS140-2 standards, if FIPS140 compliance is mandated and a stronger encryption standard is required, then a third party encryption system must be used.

Third party encryption resources for Oracle include:

Relational Database Consultants;
http://www.relationalwizards.com/html/ora_products.html

Semantica Software;
http://www.semantica.nl/en/products/plcrypt/about.html

NEC Tricryption
http://www.necsam.com/tricryption

Ingrian Networks;
http://www.ingrian.com/products/#prodline

Each of these encryption providers products encrypt the databases at a file, row or field level without requiring the setting of the SQLNET.FIPS_140 value to TRUE or the setting of the SQLNET.ENCRYPTION_TYPES_SERVER to DES|DES140. They also offer encryption using 3DES, AES, and additional algorithms.

## Appendix D – Waivers and Exceptions

### Waiver or exception procedure
The goal for the waiver or exception to the baseline is not to exempt or negate security considerations, but rather provide a means for the maintenance of the security standards outside of the mandated means.

### Compensation for the waiver or exemption
The steps taken to compensate for the waiver or the exemption should equal or surpass the standard for security of the affected element. Further, the compensation must not be in conflict with or any way jeopardize existing security measures.

### Documentation of the waiver or exception
Because security methodologies are both contextual and interrelated, a waiver or exception cannot exist in isolation from the scope of other security methodologies and cannot be executed without at least the awareness and/or understanding of all other security agents functioning under the same security hierarchy. Toward insuring all other security agents are informed of the waiver or exception, detailed documentation of the waiver or exception should be made and circulated. At a minimum the documentation should include a detailed description of the justification/s, nature, scope, duration, and means of compensation for the waiver or exception.

### Justification
By their nature, the justifications for waivers or exception cannot be predicted. Reasons might include situations where compliance with the standard would adversely affect the accomplishment of the mission of the computer system, or where compliance with the standard would cause a major financial impact on the operator, which is not offset by concurrent or subsequent cost of a security breach.

### Nature
The nature of the waiver or exception delineates where within the hierarchy of software, hardware, physical, infrastructure, or personnel the exemption will be effected. If the deviation from the standards of the baseline is of a scope to cover multiple elements, then the effect on each element must be documented.

### Scope
The scope of the waiver or exception provides the range to which operating system/s, application/s, machine/s, network/s, person/s or procedures will be covered by the exemption.

### Compensation
The compensation of the waiver or exception details what will be put in place as a substitute for the mandated settings, procedures or protocols. The explanation of the compensation must include how it will meet or exceed the existing standards for security.

### Duration
The duration of the waiver or exception explains how long the exemption will be in effect.

### Importance of duration
In almost all cases, a waiver or exception should not be accepted as a static modification, but should be considered as an exemption of fixed duration that will be resolved by the restoration of the software, hardware, procedure, personnel, or other security element/s to the defined security standard.

### Steps at the expiration of the duration

At the expiration of the duration, the waiver or exception to should be reviewed for means to return the software, hardware, procedure, personnel, or other security element/s to the defined security standard. This is not a renewal process, but must include a re-examination of the justification, nature, scope, and duration of the waiver or exception.

**Appendix E – Using Enterprise Manager Grid Control for Patch Management and Policy Violations**

The Oracle 10g Enterprise Manager Grid Control application has two functions directly related to securing Oracle and its host. If the Oracle Enterprise Manager Grid Control application is deployed, follow these recommendations. For more detailed information of this functionality please refer to the Oracle documentation, *Oracle® Enterprise Manager Concepts 10g Release 1 (10.1) Part No. B12016-02* and *Oracle® Enterprise Manager Advanced Configuration 10g Release 1 (10.1) Part No. B12013-03*.

**Patching Setup:**

The Oracle 10g Enterprise Manager Grid Control application can be set up to automatically access Oracle MetaLink to search for and download any new patches availabel for your Oracle install. The administrator can then schedule and apply the patch(es) to any host in the enterprise.

**Policy Violations:**

The Oracle 10g Enterprise Manager Grid Control application can show policy violations for any database or host in the enterprise. The violations can be fixed or ignored so they will not show up in future reports.