the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Oracle Database Server 11g

Version 1.0.0
September 2008

Leader:
Adam Cecchetti
Leviathan Security Group, Inc.

Copyright 2001-2008, The Center for Internet Security
http://cisecurity.org
cis-feedback@cisecurity.org

Table of Contents

Agreed Terms of Use 1
Introduction 4
1. Operating System Specific Settings 5
2. Installation and Patch 12
3. Oracle Directory and File Permissions 20
4. Oracle Parameter Settings 33
5. Encryption Specific Settings 55
6. Startup and Shutdown 67
7. Backup and Disaster Recovery 68
8. Oracle Profile (User) Setup Settings 72
9. Oracle Profile (User) Access Settings 82
10. Enterprise Manager / Grid Control / Agents 108
11. Specific Systems 111
12. General Policy and Procedures 113
13. Auditing Policy and Procedures 137
Appendix A – Additional Settings (not scored) 148
Appendix B – Acknowledgments 154
Appendix C – Waivers and Exceptions 155
Appendix D – Using Enterprise Manager Grid Control for Patch and Policy Management 156
Appendix E -- Change History 156

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 available" 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.

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 document is derived from research conducted utilizing the Oracle 11g program, the Oracle's Technology Network (otn.oracle.com), various published books and the Oracle 11g Database Security Guidelines. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an Oracle 11g database environment. 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.

Applicable items were verified and tested against an Oracle 11g default install on a Redhat Enterprise Sever 5. The Oracle version used was 11.1.0.6.0.Where the default setting is less secure than 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. Linux settings should translate to other varieties of Linux, but were only tested against RHEL5. If any differences are found, please contact the CIS team.

Under the Level heading, scoring data has been included:

S – To be scored.
N – Not to be scored.
R – Reportable, but not to be scored.

This information indicates how the CIS Oracle Scoring tool will handle this specific setting.

The Level column indicates the following:

- Level 1 settings are generally considered "safe" to apply to most systems. The use of these configuration recommendations is not likely to have a negative impact on performance or functionality.
- Level 2 settings provide a higher level of security, but will result in a negative impact to performance and functionality.

It is extremely important to conduct testing of security configurations on non-production systems prior to implementing them on production systems.

1. Operating System Specific Settings

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.01	Windows platform	Do not install Oracle on a domain controller	**Rationale:** This action will reduce the attack surface of the Domain Controller and the Oracle server. **Remediation:** Create a standalone server for the Oracle install. **Audit:** Execute the following WMI Query: `Select DomainRole from \ Win32_ComputerSystem` If the above returns a `4` or `5` the system is a Domain Controller.	√		1 S
1.02	Windows Oracle Local Account	Use Restricted Service Account (RSA)	**Rationale:** Adding an additional administrative account to the system increases the attack surface of the Windows server. Creating a local administrator with restricted access mitigates this risk. **Remediation:** 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. **Audit:** None	√		1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.03	Windows Oracle Domain Account	Use Restricted Service Account (RSA)	**Rationale:** 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, i.e., restricted domain user account. **Remediation:** Add the account to the local administrators group on the server running the Oracle services. **Audit:** None	√		1 N
1.04	Windows Oracle Account	Deny Log on Locally Right	**Rationale:** The RSA must have limited access requirements. **Remediation:** Deny the Log on Locally right to the RSA. **Audit:** Ensure the Oracle account is listed beneath `Local Policies\User Rights Assignments\Deny Log on Locally` in the Windows Local Security Policy	√		1 S
1.05	Windows Oracle Domain Global Group	Create a global group for the RSA and make it the RSA's primary group	**Rationale:** The RSA account should not have access to resources that all domain users need to access. **Remediation:** Do not assign any rights to the group. **Audit:** None	√		1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.06	Windows Oracle Account Domain Users Group Membership	Remove the RSA from the Domain Users group	**Rationale:** The RSA must have limited access requirements. Granting the RSA domain level privileges negates the purpose of the RSA. **Remediation:** Remove the RSA from the Domain Users group. **Audit:** On the domain controller, execute the following: `dsget user <OracleUserDN> -memberof` Ensure `Domain Users` is not listed. For more information on the `dsget` command, see http://technet.microsoft.com/en-us/library/cc755876.aspx	√		1 S
1.07	Windows Oracle Domain Network Resource Permissions	Verify and set permissions	**Rationale:** The RSA must have limited access requirements. **Remediation:** Give the appropriate permissions to the RSA or global group for the network resources that are required. **Audit:** None	√		1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.08	Windows Oracle Domain Account Logon to… Value	Limit to machine running Oracle services	**Rationale:** The RSA must have limited access requirements and be limited to authenticating to the Oracle server. **Remediation:** Configure the RSA to only log on to the computer that is running the Oracle services. **Audit:** None	√		1 S
1.09	Windows Program Folder Permissions	Verify and set permissions	**Rationale:** The Oracle program installation folder must allow only limited access. Global access or unrestricted folder permissions will allow an attacker to alter Oracle resources and possibly compromise the security of the Oracle system. **Remediation:** Remove permissions for the Users group from the `%ProgramFiles%\Oracle` folder. **Audit:** Execute the following command: `cacls "%ProgramFiles%\Oracle"` and ensure `BUILTIN\Users` is not listed.	√		1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.10	Windows Oracle Registry Key Permissions	Verify and set permissions	**Rationale:** Access to the `Oracle` registry key must be limited to those users that require it. Unrestricted access to the `Oracle` registry entries will allow non-administrative users to alter settings and create an insecure environment. **Remediation:** 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. Give read permissions to those users that require it. **Audit:** In `regedit`, browse to the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE` key, right click, select `Permissions`, and ensure the `Users` group is not granted access.	√		1 S
1.11	Windows Oracle Registry Key Setting	Set `OSAUTH_PREFIX_DOMAIN` registry value to `TRUE`	**Rationale:**This configuration strengthens the authentication process by requiring that the domain name be part of the username for externally authenticated accounts. **Remediation:** Set the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES\OSAUTH_PREFIX_DOMAIN` value to `TRUE` Note: This is the default configuration. **Audit:** In `regedit`, ensure the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES\OSAUTH_PREFIX_DOMAIN` value set to `TRUE`.	√		1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.12	Windows registry	`Set USE_SHARED_SOCKET` registry value to `TRUE`	**Rationale:** Confines client connections to the same port as the listener. This allows connection and firewall management to be performed in a more consistent and refined manner. **Remediation:** Set the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME<#>\USE_SHARED_SOCKET` registry key to `TRUE`. 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. Note: This is the default configuration. **Audit:** In `regedit`, Ensure the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME<#>\USE_SHARED_SOCKET` registry key is set to `TRUE`.	√		2 S
1.13	Oracle software owner host account	Lock account	**Rationale:** Locking the user account will deter attackers from leveraging this account in brute force authentication attacks. **Remediation:** 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. **Audit:** `grep –i account_name /etc/password`		√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score
1.14	All associated application files	Verify permissions	**Rationale:** Allowing improper access to binaries that directly interface with the Oracle database adds unnecessary risk and increases the attack surface of the database. **Remediation:** 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 data files. **Audit:** None	√	√	2 N

2. Installation and Patch

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
2.01	Installation	Try to ensure that no other users are connected while installing Oracle 11g.	**Rationale:** The Oracle 11g installer application could potentially create files, accounts, or setting with public privileges. An attacker may leverage these to compromise the integrity of the system or database before the installation is complete. **Remediation:** The Oracle 11g 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 11g. 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. If possible install Oracle while the server is disconnected from the network. If the server must be installed remotely temporarily stop inbound remote connections via administration protocols ex. SSH, Terminal Service, VNC. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
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.	**Rationale:** Using outdated or unpatched software will put the Oracle database and host system at unnecessary risk and violates security best practices. **Remediation:** 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 **Audit:** `opatch lsinventory -detail`	√	√	1 S
2.03	Minimal Install	Ensure that only the Oracle components necessary to your environment are selected for installation.	**Rationale:** Installing components that are not used increases the attack surface of the database server. **Remediation:** Install only components needed to satisfy operational requirements. Remove components that may have been installed during a previous installation but are not required. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
2.04	tkprof	Remove from system	**Rationale:** The `tkprof` utility must be removed from production environments; it is a powerful tool for an attacker to find issues in the running database. If `tkprof` must remain on the production system, it must be protected by proper permissions. **Remediation:** 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. Go to the $`ORACLE_HOME/bin` directory and remove or change the permissions of the utility. **Audit:** `$ORACLE_HOME/bin/tkprof`	√	√	1 S
2.05	listener.ora	Change default name of listener	**Rationale:** The listener must not be called by the default name as it is commonly known. A distinct name must be selected. **Remediation:** Edit `$ORACLE_HOME/network/admin/listener.ora` and change the default name. **Audit:** `grep default $ORACLE_HOME/network/admin/listener.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

2.06	listener.ora	Use IP addresses rather than hostnames	**Rationale:**
			IP addresses instead of host names in the listener.ora file must be used. This prevents a compromised or spoofed DNS server from causing Oracle outages or man in the middle attacks. Hostnames are used by default.
			
			Remediation:
			Edit
			`$ORACLE_HOME/network/admin/listener.ora`
			and replace DNS names with IP addresses.
			
			Audit:
			`grep -i HOST $ORACLE_HOME/network/admin/listener.ora`
				√	√	2
						S

2.07	otrace	Disable	**Rationale:** otrace can leak sensitive information useful for an attacker. **Remediation:** 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. Note that this directory is installed for the Enterprise Manager Grid Controller. It is not installed with a default 11g database installation. **Audit:** `ls $ORACLE_HOME/otrace/admin/*.dat`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
2.08	Listener password	Use OS Authentication	**Rationale:** It is more secure to use OS authentication as setting a password on the listener will enable remote administration of the listener. **Remediation:** OS Authentication is enabled by default.. If additional users require remote access to the listener, set an encrypted password using the `set password` command via the `lsnrctl` tool. Be aware, setting a password in the listener.ora file will set an unencrypted password on the listener. **Audit:** `grep -i PASSWORD \ $ORACLE_HOME/network/admin/listener.ora`	√	√	1 S
2.09	Default Accounts (created by Oracle)	The following actions are recommended in order of preference for default accounts: 1. Drop the user 2. Lock the user account 3. Change the default password	**Rationale:** The default Oracle installation locks and expires the installation accounts. These accounts should be left locked and expired unless absolutely necessary. Check to ensure these accounts have not been unlocked. **Remediation:** Lock and expire the system accounts. **Audit:** `SELECT * FROM DBA_USERS_WITH_DEFPWD;`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

2.10	OEM objects	Remove if OEM not used	**Rationale:**
			Removing the OEM will reduce the Oracle attack surface.
			
			Remediation:
			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.
			
			`$ORACLE_HOME/rdbms/admin/catnsmp.sql`
			`rm $ORACLE_HOME/bin/dbsnmp`
			
			Audit:
			`ls –al $ORACLE_HOME/bin/dbsnmp`
				√	√	2
						S

2.11	listener.ora	Change standard ports	**Rationale:**
			Standard ports are used in automated attacks and by attackers to verify applications running on a server.
			
			Remediation:
			Alter the `listener.ora` file and change the PORT setting.
			
			Note: This may break applications that hard code the default port number.
			
			Audit:
			`grep 1521 \`
			`$ORACLE_HOME/network/admin/listener.ora`
			
			`grep 1526 \`
			`$ORACLE_HOME/network/admin/listener.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

2.12	Third party default passwords	Set all default account passwords to non-default strong passwords	**Rationale:**
			When installed, some third party applications create well-known default accounts in an Oracle database.
			
			Remediation:
			The default passwords for these accounts must be changed or the account must be locked.
			
			`ALTER USER <USERNAME> IDENTIFIED BY <PASSWORD>;`
			`ALTER USER <USERNAME> ACCOUNT LOCK PASSWORD EXPIRE;`
			
			Audit:
			`SELECT * FROM DBA_USERS_WITH_DEFPWD;`
			`SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;`
				√	√	2
						S

2.13	Service or SID name	Non-default	**Rationale:**
			Do not use the default SID or service name of ORCL. It is commonly know and used in many automated attacks.
			
			Remediation:
			Alter the listener.ora file SID setting to a value other than the default. Ensure the SID is at least 7 characters long to prevent successful brute force attacks.
			
			Audit:
			`grep -i ORCL \`
			`$ORACLE_HOME/network/admin/listener.ora`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
2.14	Oracle Installation	Oracle software owner account name NOT ‘oracle’	**Rationale:** Do not name the Oracle software owner account ‘oracle’ as it is very well known and can be leveraged by an attacker in a brute force attack. **Remediation:** Change the user used for the oracle software. **Audit:** `grep -i oracle /etc/password`	√	√	2 S
2.15	Oracle Installation	Separate users for different components of Oracle	**Rationale:** The user for the intelligent agent, the listener, and the database must be separated. This setup may cause unknown or unexpected errors and should be extensively tested before deployment into production. This is not recommended for Windows environments. **Remediation:** For Unix systems, create unique user accounts for each Oracle process/service in order to differentiate accountability and file access controls. **Audit:** None		√	2 N

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.

Note: Some Unix operating systems make use of extended ACL's which may contain permissions more secure then the recommendations listed here. Please be sure to fully examine and test permissions before implementing them on production systems.

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
3.01	Files in `$ORACLE_HOME/bin`	Verify and set ownership	**Rationale:** All files in the `$ORACLE_HOME/bin` must be owned by the Oracle software account to prevent a system-wide compromise in the event the Oracle account is compromised. In Windows, this account must be part of the Administrators group. **Remediation:** Change the ownership of the binaries to the appropriate account. **Audit:** `ls -al $ORACLE_HOME/bin/*`	√	√	1 S

3.02	Files in `$ORACLE_HOME/bin`	Permissions set to 0755 or less	**Rationale:**
			Incorrect permissions could allow an attacker to replace a binary with a malicious version.
			
			Remediation:
			All files in the `$ORACLE_HOME/bin` directory must have permissions set to 0755 or less.
			
			`chmod 0755 $ORACLE_HOME/bin/*`
			
			Audit:
			`ls -al $ORACLE_HOME/bin/*`
					√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.03	Files in `$ORACLE_HOME` (not including `$ORACLE_HOME/bin`)	Permissions set to `0750` or less on Unix systems	**Rationale:**
			Incorrect permissions could allow an attacker to execute or replace a command with a malicious version.
			
			Remediation:
			All files in `$ORACLE_HOME` directories (except for `$ORACLE_HOME/bin`) must have permission set to 0750 or less.
			
			`chmod 750 $ORACLE_HOME/*`
			
			Audit:
			`ls –al $ORACLE_HOME`
					√	1
						S

3.04	Oracle account .profile file	Unix systems umask 022	**Rationale:** Regardless of where the `umask` is set, `umask` must be set to `022` before installing Oracle. Ad improper `umask` can lead to unrestrictive permissions and open the oracle server file system to attack. **Remediation:** Ensure the `umask` value is `022` for the owner of the Oracle software before installing Oracle. **Audit:** `umask`		√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.05	init.ora	Verify and restrict permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group. If unprivileged users can alter the init.ora configuration the security of the oracle server can be compromised.
			
			Remediation:
			`chgrp oracle_grp init.ora`
			`chown oracleuser init.ora`
			`chmod 644 init.ora`
			
			Audit:
			`ls -al $ORACLE_HOME/dbs/init.ora`
				√	√	1
						S

3.06	spfile.ora	Verify and restrict permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group. If unprivileged users can alter the spfile.ora configuration the security of the oracle server can be compromised.
			
			Remediation:
			`chgrp oracle_grp spfile.ora`
			`chown oracleuser spfile.ora`
			`chmod 640 spfile.ora`
			
			Audit:
			`ls -al $ORACLE_HOME/dbs/spfile.ora`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.07	Database datafiles	Verify and restrict permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group. If unprivileged users can read or alter the `dbs` files the security of the oracle server can be compromised.
			
			Remediation:
			`chown oracleuser $ORACLE_HOME/dbs/*`
			`chgrp oraclegroup $ORACLE_HOME/dbs/*`
			
			Audit:
			`ls -al $ORACLE_HOME/dbs/*`
				√	√	1
						S

3.08	init.ora	Verify permissions of file referenced by `ifile` parameter	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group. 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.
			
			Remediation:
			`chmod 750 ifile`
			`chown oracleuser.oraclegroup ifile`
			
			Audit:
			`grep ifile init.ora`
			`ls -al <result>`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.09	init.ora	`audit_file_dest` parameter settings	**Rationale:**
			The destination for the audit file must be set to a valid directory owned by oracle and set with owner read/write permissions only.
			
			Remediation:
			`chmod 600 auditfile`
			`chown oracleuser.oraclegroup auditfile`
			
			Audit:
			`grep -i audit_file_dest init.ora`
			`ls -al <result>`
				√	√	1
						S

3.10	init.ora	`diagonostic_dest` parameter settings	**Rationale:**
			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.
			
			Remediation:
			`chmod 660 diag_file`
			`chown oracleuser.oraclegroup diag_file`
			
			Audit:
			`grep -i diagonostic_dest init.ora`
			`ls -al <result>`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.11	init.ora	`control_files` parameter settings	**Rationale:**
			The permissions must be restricted to only the owner of the Oracle software and the `dba` group.
			
			Remediation:
			`chmod 640 control_file`
			`chown oracleuser.oraclegroup control_file`
			
			Audit:
			`grep -i control_files init.ora`
			`ls -al <result>`
			`select name from V$controlfile;`
				√	√	1
						S

3.12	init.ora	`log_archive_dest_n` parameter settings	**Rationale:**
			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.
			
			Remediation:
			Default is " " (A null string) for all. Must configure and set paths, then ensure those directories are secure.
			
			`chmod  750 file_file_dest`
			`chown oracleuser.oraclegroup \`
			`log_file_dest`
			
			Audit:
			`grep -i log_archive_dest init.ora`
			`ls -al <result>`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.13	Files in `$ORACLE_HOME/network/admin` directory	Verify and set permissions	**Rationale:**
			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.
			
			Remediation:
			`chmod 644 $ORACLE/network/admin/*`
			`chown oracleuser.oraclegroup \`
			`$ORACLE_HOME/network/admin/*`
			
			Audit:
			`ls -al $ORACLE_HOME/network/admin/*`
				√	√	1
						S

3.14	sqlnet.ora	Verify and set permissions with read permissions for everyone.	**Rationale:**
			The `sqlnet.ora` contains the configuration files for the communication between the user and the server including the level of required encryption.
			
			Remediation:
			`chmod 644 sqlnet.ora`
			`chown oracleuser.oraclegroup sqlnet.ora`
			
			Note: If encryption is used, the key is stored in the parameter `SQLNET.CRYPTO_SEED` in the `sqlnet.ora` file. In such scenarios, access to this file should be limited.
			
			Audit:
			`ls –al sqlnet.ora`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.15	sqlnet.ora	`log_directory_client` parameter settings	**Rationale:**
			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.
			
			Remediation:
			`chmod 640 log_directory_client`
			`chown oracleuser.oraclegroup \`
			`log_directory_client`
			
			Audit:
			`grep -i log_directory_client sqlnet.ora`
				√	√	1 S

3.16	sqlnet.ora	`log_directory_server` parameter settings	**Rationale:**
			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.
			
			Remediation:
			`chmod 640 log_directory_client`
			`chown oracleuser.oraclegroup \`
			`log_directory_client`
			
			Audit:
			`grep -i log_directory_client sqlnet.ora`
				√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.17	sqlnet.ora	`trace_directory_client` parameter settings	**Rationale:**
			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 read for the dba group.. By default this is not set. Be aware, this is usually set to `$ORACLE_HOME/network/trace`, with permissions set as:
			
			Remediation:
			`chmod 640 log_directory_client`
			`chown oracleuser.oraclegroup \`
			`log_directory_client`
			
			Audit:
			`grep -i trace_directory_client sqlnet.ora`
				√	√	1
						S

3.18	sqlnet.ora	`trace_directory_server` parameter settings	**Rationale:**
			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 read for the `dba` group.
			
			By default this is not set. Be aware, this is usually set to `$ORACLE_HOME/network/trace`.
			
			Remediation:
			`chmod 640 trace_directory_server`
			`chown oracleuser.oraclegroup`
			`trace_directory_server`
			
			Audit:
			`grep -i trace_directory_server sqlnet.ora`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.19	listener.ora	Verify and set permissions	**Rationale:**
			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.
			
			Remediation:
			`chmod 660 \`
			`$ORACLE_HOME/network/admin/listener.ora`
			
			`chown oracleuser.oraclegroup \`
			`$ORACLE_HOME/network/admin/listener.ora`
			
			Audit:
			`ls -al \`
			`$ORACLE_HOME/network/admin/listener.ora`
				√	√	1
						S

3.20	listener.ora	`log_file_listener` parameter settings	**Rationale:**
			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 read for the `dba` group. By default this is not set. Be aware, this is usually set to `$ORACLE_HOME/network/log/listener.log`.
			
			Remediation:
			`chmod 640 \`
			`$ORACLE_HOME/network/log/listener.log`
			
			`chown oracleuser.oraclegroup \`
			`$ORACLE_HOME/network/log/listener.log`
			
			Audit:
			`grep -i log_file_listener \`
			`$ORACLE_HOME/network/admin/listener.ora`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.21	listener.ora	`trace_directory_listener_name` parameter settings	**Rationale:**
			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.
			
			Remediation:
			`chmod 660 trace_dir`
			`chown oracleuser.oraclegroup trace_dir`
			
			Audit:
			`grep -i trace-directory \`
			`$ORACLE_HOME/network/admin/listener.ora`
				√	√	1 S

3.22	listener.ora	`trace_file_listener_name` parameter settings	**Rationale:**
			This file must be owned by the Oracle account and permissions restricted to read/write only for the owner and `dba` group. By default this is not set. Be aware, this is usually set to `$ORACLE_HOME/network/trace`.
			
			Remediation:
			`chown oracleuser.oraclegroup \`
			`$ORACLE_HOME/network/trace`
			`chmod 660 $ORACLE_HOME/network/trace`
			
			Audit:
			`grep -i trace_file \`
			`$ORACLE_HOME/network/admin/listener.ora`
			`ls –al <result>`
				√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.23	sqlplus	Verify and set permissions	**Rationale:**
			The permissions of the binaries for `sqlplus` on the server must be restricted to the owner of the Oracle software and the `dba` group.
			
			Remediation:
			`chown oracleuser.oraclegroup sqlplus`
			`chmod 750 sqlplus`
			
			Audit:
			`which -a sqlplus`
			`ls -al <result(s)>`
				√	√	1
						S

3.24	.htaccess	Verify and set permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group.
			
			Remediation:
			`chown oracleuser.oraclegroup .htaccess`
			`chmod 644 .htaccess`
			
			Audit:
			`ls –al .htaccess`
			
			Note: Only applicable for environments using the Oracle HTTP Server. Additionally, ensure all configuration changes have been made within `.htaccess` prior to implementing this recommendation.
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

3.25	dads.conf	Verify and set permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group.
			
			Remediation:
			`chown oracleuser.oraclegroup dads.conf`
			`chmod 644 dads.conf`
			
			Audit:
			`ls –al dads.conf`
			
			Note: Only applicable for environments using the Oracle HTTP Server. Additionally, ensure all configuration changes have been made within `dads.conf` prior to implementing this recommendation.
				√	√	1
						S

3.26	xsqlconfig.xml	Verify and set permissions	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and the `dba` group.
			
			Remediation:
			`chown oracleuser.oraclegroup \`
			`xsqlconfig.xml`
			`chmod 640 xsqlconfig.xml`
			
			Audit:
			`ls -al \`
			`$ORACLE_HOME/xdk/admin/XSQLConfig.xml`
				√	√	1
						S

4. Oracle Parameter Settings

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

4.01	init.ora	`_trace_files_public= FALSE`	**Rationale:**
			Prevents users from having the ability to read trace files which may contain sensitive information about the running Oracle instance. This is an internal Oracle parameter. Do NOT use it unless instructed to do so by Oracle Support.
			
			Remediation:
			`Set _trace_files_public= FALSE`
			
			Note: Default is `FALSE`.
			
			Audit:
			`grep -i _trace_files_public init.ora`
				√	√	1
						S

4.02	init.ora	`global_names= TRUE`	**Rationale:** This parameter ensures that Oracle will check that the name of a database link is the same as that of the remote database. Default is `TRUE`. **Remediation:** Set `global_names= TRUE` in `init.ora` **Audit:** `grep -i global_names init.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.03	Init.ora	`remote_os_authent=FALSE`	**Rationale:** This setting has been deprecated, however is maintained for backwards compatibility. If this setting is used it is recommended to be set to `FALSE`. `remote_os_authent` will allow a user that is authenticated to the network domain to access the database without DB credentials. **Remediation:** Set `remote_os_authent=FALSE`. **Audit:** `grep -i remote_os_authent init.ora`	√	√	1 S
4.04	init.ora	`remote_os_roles= FALSE`	**Rationale:** Connection spoofing must be prevented. Default is `FALSE`. **Remediation:** Set `remote_os_roles= FALSE`. **Audit:** `grep -i remote_os_roles init.ora`	√	√	1 S
4.05	init.ora	`remote_listener=""` (A null string)	**Rationale:** Prevent the use of a listener on a remote machine separate from the database instance. **Remediation:** Set `remote_listener=""`. **Audit:** `grep -i remote_listener init.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.06	init.ora	`audit_trail` parameter set to `OS, DB, DB_EXTENDED, XML, or XML, EXTENDED`	**Rationale:** 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 if set to `DB or DB_EXTENDED`. Even with the `audit_trail` value set to `FALSE`, an audit session will report, "Audit succeeded." The default is `DB`. **Remediation:** Alter the `init.ora` file and set `audit_trail=OS` **Audit:** `grep -i audit_trail init.ora`	√	√	1 S
4.07	init.ora	`os_authent_prefix=""` (A null string)	**Rationale:** OS roles are subject to control outside the database. The duties and responsibilities of DBAs and system administrators must be separated. It must be set to limit the external use of an account to an `IDENTIFIED EXTERNALLY` specified user. **Remediation:** Set `os_authent_prefix=""` **Audit:** `grep -i os_authent_prefix init.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.08	init.ora	`os_roles=FALSE`	**Rationale:** `os_roles` allows externally created groups to be used to manage database roles. This can lead to misaligned or inherited permissions. **Remediation:** Set `os_roles=FALSE` **Audit:** `grep -i os_roles init.ora`	√	√	1 S
4.09	init.ora	Avoid using `utl_file_dir` parameters	**Rationale:** Do not use the `utl_file_dir` parameter directories created with `utl_file_dir` as they can be read and written to by all users. Specify directories using `CREATE DIRECTORY` which requires granting of privileges to each user. This function has been deprecated since version 9.2 migration is recommended. **Remediation:** Use `CREATE DIRECTORY` **Audit:** `grep -i utl_file_dir init.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.10	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.	**Rationale:** 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. **Remediation:** Set LOG_ARCHIVE_DUPLEX_DEST to a valid, properly secured, directory. **Audit:** `grep -i log_archive_duplex_dest init.ora`	√	√	1 S
4.11	init.ora	Specify redo logging must be successful. Use "LOG_ARCHIVE_MIN_SUCCEED_DEST" to ensure the successful logging of the redo files.	**Rationale:** Specifying that the logging must succeed in one or more locations ensures redundancy of the redo logs. **Remediation:** Set LOG_ARCHIVE_MIN_SUCCEED_DEST to 1 or greater. **Audit:** `grep -i LOG_ARCHIVE_MIN_SUCCEED_DEST \ init.ora`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.12	init.ora	`sql92_security= TRUE`	**Rationale:** 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. WARNING: This will likely result in many applications failing and should not be enabled in production without thorough testing. **Remediation:** Set `sql92_security= TRUE` **Audit:** `grep -i sql92_security init.ora`	√	√	2 S
4.13	listener.ora	`admin_restrictions_`*`listener_name`*`=on`	**Rationale:** Replace `listener_name` with the actual name of your listener(s) for this parameter setting. This requires the administrator to have write privileges to listener.ora. This setting will cause the listener to refuse set commands that alter its parameters without a restart of the listener. Not set and turned off by default. **Remediation:** Set `admin_restrictions_listener_name = on` **Audit:** `grep -i admin_restrictions listener.ora`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.14	listener.ora	`logging_listener=ON`	**Rationale:** Logging of all listener actions will create an audit trail in the event that a listener is attacked or needs to be debugged. This setting is not set, but is enabled by default. **Remediation:** Set `logging_listener=ON` **Audit:** `grep -i logging_listener listener.ora`	√	√	1 S
4.15	SQL key word “NOLOGGING”	Log listener actions not set, but turned on by default.	**Rationale:** Malicious code can be executed without an audit trail under the key word `NOLOGGING`. **Remediation:** Search applications and SQL files for the usage of the `NOLOGGING` keyword. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.16	init.ora	o7_dictionary_accessibility= FALSE	**Rationale:** This is a database initialization parameter that controls access to objects in the SYS schema. Set this to FALSE to prevent users with EXECUTE ANY PROCEDURE and SELECT ANY DICTIONARY from accessing objects in the SYS schema. If access to these objects is required, the following roles can be assigned, SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE, DELETE_CATALOG_ROLE. If set to TRUE, accounts with "ANY" privileges could get access to objects in the SYS schema. Default setting is FALSE. **Note:** In Oracle Applications 11.5.9 and lower, O7_DICTIONARY_ACCESSIBILITY must be set to TRUE. This is required for proper functioning of the application and Oracle does not support setting it to FALSE. In Apps 11.5.10 and higher, O7_DICTIONARY_ACCESSIBILITY should be set to FALSE. See Oracle Metalink Note ID 216205.1 for more information. **Remediation:** Set o7_dictionary_accessibility= FALSE **Audit:** grep –i o7_dictionary_accessibility \ init.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

4.17	spfile<sid>.ora	Remove the following from the `spfile`:
		`dispatchers= (PROTOCOL= TCP) (SERVICE= <oracle_sid>XDB)`
			Rationale:
			This will disable default ports ftp: 2100 and http: 8080. Removing the `XDB` ports will reduce the attack surface of the Oracle server. It is recommended to disable these ports if production usage is not required.
			
			Remediation:
			Remove the following from `spfile`:
			
			`dispatchers= (PROTOCOL= TCP)(SERVICE= <oracle_sid>XDB)`
			
			Audit:
			`grep -i XDB spfile<sid>.ora`
				√	√	2
						S

4.18	Init.ora or spfile<sid>.ora	`AUDIT_SYS_OPERATIONS =TRUE`	**Rationale:** Auditing of the users authenticated as the `SYSDBA` or the `SYSOPER` provides an oversight of the most privileged of users. 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`. **Remediation:** Set AUDIT_SYS_OPERATIONS=TRUE. The default value is `FALSE` within `spfile`. Set `AUDIT_FILE_DEST` to your designated logging directory. Windows: Default is `Event Viewer` log file Unix: Default is `$ORACLE_HOME/rdbms/audit` By default this is set in `spfile`. **Audit:** `grep -i AUDIT_SYS_OPERATIONS init.ora`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.19	listener.ora	`inbound_connect_timeout_`*`listener`*`=2`	**Rationale:** Allowing inbound connections to hold open half connections consumes database resources and can lead to denial of service. Set the initial value low and adjust upward if normal clients are unable to connect within the time allocated. **Remediation:** Set `inbound_connect_timeout_listener=2` **Audit:** `grep -i inbound_connect_timeout \ listener.ora`	√	√	2 S

4.20	sqlnet.ora	`tcp.validnode_checking= YES`	**Rationale:**
			This parameter enables the listener to check incoming connections for matches in the invited and excluded nodes list.
			
			Remediation:
			`Set tcp.validnode_checking=YES`
			in `$ORACLE_HOME/network/admin/sqlnet.ora`.
			
			Note: The default value is `No`
			
			Audit:
			`grep -i tcp.validnode_checking sqlnet.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

4.21	sqlnet.ora	Set `tcp.invited_nodes` to valid values	**Rationale:**
			This creates a list of trusted nodes that can connect to the listener. The `excluded_nodes` value is ignored if this is set and a default deny policy is created only allowing the listed trusted nodes to connect to the listener.
			
			Remediation:
			Use IP addresses of authorized hosts to set this parameter in the sqlnet.ora file.
			
			Set `tcp.invited_nodes` to valid values
			`tcp.invited_nodes =(10.1.1.1, 10.1.1.2)`
			
			Audit:
			`grep -i tcp.invited_nodes sqlnet.ora`
			
			Note: This is not set by default.
				√	√	2
						S

4.22	sqlnet.ora	Set `tcp.excluded_nodes` to valid values	**Rationale:** Excluded nodes will prevent malicious or untrusted hosts from connecting to the listener. **Remediation:** 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 and only hosts specified in the `invited_nodes` will be allowed to connect to the listener. Set `tcp.excluded_nodes` to valid values **Audit:** `grep -i tcp.excluded_nodes sqlnet.ora`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.23	sqlnet.ora	`sqlnet.inbound_ connect_timeout=3`	**Rationale:** Allowing inbound connections to hold open half connections consumes database resource and can lead to denial of service. Suggestion is to set to a low initial value and adjust upward if normal clients are unable to connect within the time allocated. **Remediation:** Set `sqlnet.inbound_connect_timeout=3` **Audit:** `grep -i inbound_connect_timeout \ sqlnet.ora`	√	√	2 S
4.24	sqlnet.ora	`sqlnet.expire_time= 10`	**Rationale:** If this is not set in the sqlnet.ora file, the default is never to expire. Allowing a connection to idle indefinitely will consume system resources leading to a denial of service. It is recommended to set this to a low value initially, then increase if clients experience timeout issues. **Remediation:** Set `sqlnet.expire_time= 10` **Audit:** `grep -i expire_time sqlnet.ora`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

4.25	Accounts	Lock account access for application schema owners	**Rationale:**
			Lock the account for the application schema owner. Users must not connect to the database as the application owner.
			
			Remediation:
			`ALTER USER <USERNAME> ACCOUNT LOCK PASSWORD EXPIRE`
			
			Audit:
			`SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

4.26	init.ora	`remote_login_passwordfile=none`	**Rationale:**
			Prevents remote privileged connections to the database. This suggests that remote administration should be performed by remotely logging into the database server via a secured connection. Alternately, an administrative listener could be created, the `remote_login_passwordfile` set to exclusive, and logging of the administrative listener implemented.
			
			Remediation:
			For Windows: Set `remote_login_passwordfile` setting to `none`.
			Implement remote management to a Windows based host viaTerminal Server and IPSec.
			
			For Unix: Set `remote_login_passwordfile` setting to `none`. Implement SSH or other secure shell method to remotely administer the Oracle server.
			
			Remote Administration of Oracle via Administrative Listener:
			
			Admin Listener = Required
			`remote_login_passwordfile` setting = `exclusive`
			
			Require logging be enabled for the Admin and Client Listeners if remote access is provided.
			
			Audit:
			`grep –i remote_login_passwordfile \ init.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.27	sqlnet.ora	SQLNET.ALLOWED_LOGON_VERSION=11	**Rationale:** Set the login version to the 11. The higher setting prevents logins by older version clients that do not use strong authentication to pass the login credentials. The default setting is 10,9,8. **Remediation:** SQLNET.ALLOWED_LOGON_VERSION=11 **Audit:** grep -i ALLOWED_LOGIN_VERSION sqlnet.ora	√	√	2 S
4.28	listener.ora	Use absolute paths in ENVS parameters.	**Rationale:** Allowing overly broad PATH and CLASSPATH variables could allow an attacker to leverage pathing issues and load malicious binaries or classes. **Remediation:** Remove broad path or classpath variables and ensure only absolute paths are used. **Note:** The ENVS SID_DESC parameter is not supported on Windows however the environment variables can be defined for the listener. **Audit:** grep –i ENVS listener.ora .	√	√	2 N
4.29	cman.ora	REMOTE_ADMIN=NO	**Rationale:** Ensure remote administration is not left enabled. Default is NO. **Remediation:** Set REMOTE_ADMIN = NO. **Audit:** grep –i REMOTE_ADMIN cman.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.30	listener.ora, tnsnames.ora	Disable external procedures	**Rationale:** Remove entries for external procedures from `listener.ora` or `tnsnames.ora` file. External procedures can call shared libraries on the host system from the `$ORACLE_HOME/lib` or `$ORACLE_HOME/bin` directories. This creates a dangerous condition. If not required disable their usage. **Remediation:** Remove external shared libraries from `$ORACLE_HOME/lib` **Audit:** None	√	√	2 N

4.31	init.ora	`SEC_RETURN_SERVER_RELEASE_BANNER = false`	**Rationale:**
			Ensure the oracle database is not returning complete database information to clients. Knowing the exact patch set can aid an attacker.
			
			Remediation:
			`SEC_RETURN_SERVER_RELEASE_BANNER = false`
			
			Audit:
			`grep -i \`
			`SEC_RETURN_SERVER_RELEASE_BANNER init.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.32	init.ora	DB_SECUREFILE=ALWAYS	**Rationale:** Ensure that all LOB files created by Oracle are created as SecureFiles. **Remediation:** DB_SECUREFILE=ALWAYS **Audit:** grep -i DB_SECUREFILE init.ora	√	√	2 N
4.33	init.ora	SEC_CASE_SENSITIVE_LOGON=TRUE	**Rationale:** Set Oracle database password to be case sensitive. This increases the complexity of passwords and helps defend against brute force password attacks. **Remediation:** SEC_CASE_SENSITIVE_LOGON=TRUE **Audit:** grep -i SEC_CASE_SENSITIVE_LOGO init.ora	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.34	init.ora	SEC_MAX_FAILED_LOGIN_ATTEMPTS=3	**Rationale:** Set the maximum number of failed login attempts to be 3 or in sync with established password policies. This will reduce the effectiveness of a password brute force attack. Note: Setting SEC_MAX_FAILED_LOGIN_ATTEMPTS to a value other than UNLIMITED may increase an attacker's ability to intentionally lockout sensitive accounts, such as those used by middle-tier applications. Given this, implementer's should consider connectivity restrictions to the Oracle instance backing the application and the determinism of usernames used by such applications. **Remediation:** SEC_MAX_FAILED_LOGIN_ATTEMPTS=3 **Audit:** grep -i SEC_MAX_FAILED_LOGIN_ATTEMPTS \ init.ora	√	√	1 S
4.35	init.ora	SEC_PROTOCOL_ERROR_FURTHER_ACTION=DELAY <seconds>or DROP<seconds>	**Rationale:** When bad packets are received from a client the server will wait the specified number of seconds before allowing a connection from the same client. This help mitigate malicious connections or DOS conditions. **Remediation:** SEC_PROTOCOL_ERROR_FURTHER_ACTION=DELAY <seconds>or DROP<seconds> **Audit:** grep –i \ SEC_PROTOCOL_ERROR_FURTHER_ACTION \ init.ora	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.36	init.ora	SEC_PROTOCOL_ERROR_TRACE_ACTION=LOG or ALERT	**Rationale:** Specify the action a database should take when a bad packet is received. TRACE generates a detailed trace file and should only be used when debugging. ALERT or LOG should be used to capture the event. Use currently established procedures for checking console or log file data to monitor these events. **Remediation:** SEC_PROTOCOL_ERROR_TRACE_ACTION= {LOG|ALERT} **Audit:** grep –i \ SEC_PROTOCOL_ERROR_TRACE_ACTION init.ora	√	√	1 S
4.37	sqlnet.ora	SEC_USER_AUDIT_ACTION_BANNER=/path/to/warning.txt	**Rationale:** A banner should be set to warn a user about the possible audit actions that are taken when using the system. Set the complete path to the file that contains the warning. **Remediation:** SEC_USER_AUDIT_ACTION_BANNER=/path/to/warning.txt **Audit:** grep –i \ SEC_USER_AUDIT_ACTION_BANNER sqlnet.ora	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.38	sqlnet.ora	SEC_USER_UNAUTHORIZED_ACCESS_BANNER=/path/to/warning.txt	**Rationale:** A banner should be set to warn a user about unauthorized access to the database that is in line with current policy or language. Set the complete path to the file that contains the warning. OCI and other custom applications must make use of this parameter before it is displayed to the user. **Remediation:** SEC_USER_UNAUTHORIZED_ACCESS_BANNER=/path/to/warning.txt **Audit:** grep -i \ SEC_USER_UNAUTHORIZED_ACCESS_BANNER \ sqlnet.ora	√	√	1 N
4.39	listener.ora	SECURE_CONTROL_listener_name=(TCPS,IPC)	**Rationale:** If remote administration of the listener is required configure the listener for secure control. If no values are entered for this parameter, the listener will accept registration request from any transport. If only IPC or TCPS is required then set the value to TCPS or IPC. **Remediation:** SECURE_CONTROL_listener_name=(TCPS,IPC) **Audit:** grep -i SECURE_CONTROL listener.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.40	listener.ora	SECURE_PROTOCOL_listener_name=(TCP,IPC)	**Rationale:** Ensure that any administration requests are accepted only over secure transport. If only IPC or TCP is required then set the value to TCPS or IPC. **Remediation:** SECURE_PROTOCOL_listener_name=(TCPS,IPC) **Audit:** grep -i SECURE_PROTOCOL listener.ora	√	√	1 S
4.41	listener.ora	SECURE_REGISTER_listener_name=(TCP,IPC)	**Rationale:** Ensure that any registration requests are accepted over secure transport. If only IPC or TCP is required then set the value to TCPS or IPC. **Remediation:** SECURE_REGISTER_listener_name=(TCPS,IPC) **Audit:** grep -i SECURE_REGISTER listener.ora	√	√	2 S
4.42	listener.ora	DYNAMIC_REGISTRATION_listener_name=OFF	**Rationale:** If DYNAMIC_REGISTRATION is turned on all registration connections are accepted by the listener. It is recommended that only static registrations be used by the listener. Turning off dynamic registration may not be possible in larger or more dynamic environments. Ensure proper testing is done before turning off dynamic registration in production. **Remediation:** DYNAMIC_REGISTRATION_listener_name=OFF **Audit:** grep –i DYNAMIC_REGISTRATION listener.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
4.43	listener.ora	EXTPROC_DLLS=ONLY	**Rationale:** Where use of external procedures is required, specify the EXTPROC_DLLS=ONLY in the parameter to limit calls to the specific DLLS. This prevents external DLLs and libraries from being loaded by the Oracle database. An attacker that can load an external library into the Oracle running instance can take control or compromise system security. If external DLLs must be used specify the ONLY parameter and an absolute path for each required DLL. **Remediation:** EXTPROC_DLLS=ONLY **Audit:** grep –i EXTPROCS_DLLS listener.ora	√	√	1 S

5. Encryption Specific Settings

Note: OAS is installed by default even if it is not licensed. Therefore, it must be configured even if it is not used.

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.01	OAS - General	Review requirement for integrity and confidentiality requirements.	**Rationale:** Only implement OAS if a local integrity/encryption policy does not already exist, e.g., IPSec or other means for providing integrity/confidentiality services. **Remediation:** Review requirement for integrity and confidentiality requirements. **Audit:** None	√	√	2 N

5.02	OAS – Encryption Type	`SQLNET.ENCRYPTION_SERVER=REQUIRED`	**Rationale:**
			This ensures that regardless of the settings on the user, if communication takes place it must be encrypted. Default is accepted.
			
			Remediation:
			`SQLNET.ENCRYPTION_SERVER=REQUIRED`
			
			Audit:
			`grep –i ENCRYPTION_SERVER sqlnet.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.03	OAS – Encryption Type	SQLNET.ENCRYPTION_CLIENT=(ACCEPTED|REQUESTED|REQUIRED)	**Rationale:** Communication is only possible on the basis of an agreement between the client and the server regarding the connection encryption. To ensure encrypted communication, set the value to REQUIRED. With the server set to REQUIRED the client must match the encryption for valid communication to take place. Default is accepted. **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. **Remediation:** SQLNET.ENCRYPTION_CLIENT=REQUIRED **Audit:** grep –i ENCRYPTION_CLIENT sqlnet.ora	√	√	2 S
5.04	OAS – FIPS Compliance	SSLFIPS_140 =TRUE	**Rationale:** For FIPS 140-2 compliance, the FIPS value must be set to TRUE. The default value for this setting is FALSE. 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. **Remediation:** SSLFIPS_140 =TRUE **Audit:** grep –i SSL_FIPS fips.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.07	OAS – Integrity Protection	Integrity check for communication between the server and the client must be established. "SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED" "SQLNET.CRYPTO_CHECKSUM_CLIENT=REQUIRED"	**Rationale:** The integrity check for communication can prevent data modifications. Two check sum algorithms are available; SHA-1 and MD5. Default is accepted. **Remediation:** Set SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED SQLNET.CRYPTO_CHECKSUM_CLIENT=REQUIRED **Audit:** grep –i CRYPTO_CHECKSUM_SERVER sqlnet.ora grep –i CRYPTO_CHECKSUM_CLIENT sqlnet.ora	√	√	2 S
5.08	OAS – Integrity Protection	Set SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA1)	**Rationale:** If possible, use SHA1 instead of MD5. MD5 has documented weaknesses and is prone to collisions. Usage of SHA-1 is recommended. Default is all. **Remediation:** Set SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA1) **Audit:** grep –i CHECKSUM_TYPES_SERVER sqlnet.ora	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.09	OAS – Oracle Wallet Owner Permissions	Set configuration method for Oracle Wallet. Ensure only the appropriate Oracle user account has access to the wallet.	**Rationale:** The Oracle service account must have access to the wallet. **Remediation:** None **Audit:** None	√	√	2 N
5.10	OAS – Oracle Wallet Trusted Certificates	Remove certificate authorities (CAs) that are not required.	**Rationale:** Trust only those CAs that are required by clients and servers. **Remediation:** Remove certificate authorities (CAs) that are not required. **Audit:** `orapki wallet display -wallet \ wallet_location`	√	√	2 S
5.11	OAS – Oracle Wallet Trusted Certificates Import	When adding CAs, verify fingerprint of CA certificates.	**Rationale:** When adding CA certificates via out-of-band methods, use fingerprints to verify the certificate. Failure to verify fingerprints can lead to compromise of the certificate chain. **Remediation:** When adding CAs, verify fingerprint of CA certificates. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

5.12	OAS – Certificate Request Key Size	Request the maximum key size available.	**Rationale:**
			Select the largest key size available that is compatible with the network environment. 2048 or 4096 are recommended sizes.
			
			Remediation:
			`orapki wallet add -wallet \`
			`wallet_location -dn user_dn -keySize 2048`
			
			Audit:
			`orapki wallet display -wallet \`
			`wallet_location`
				√	√	2
						S

5.13	OAS – Server Oracle Wallet Auto Login	Allow Auto Login for the server's Oracle Wallet	**Rationale:** For Windows Oracle database servers, SSL will not work unless Auto Login is set. **Remediation:** To enable auto login from the Oracle Wallet Manager. Choose Wallet from the menu bar. Check Auto Login. A message at the bottom of the window indicates that auto login is enabled. **Audit:** Choose Wallet from the menu bar. Check Auto Login.	√	√	2 S
5.14	OAS – SSL Tab	SSL is preferred method. If PKI is not possible, use OAS Integrity/Encryption.	**Rationale:** OAS Integrity/Encryption should only be used if required because of non-SSL clients. **Remediation:** Use OAS Integrity/Encryption only if SSL is unavailable. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

5.15	OAS – SSL Version	Set SSL version.
		`SSL_VERSION = 3.0`
			Rationale:
			Usage of the most current version of SSL is recommended older versions of the SSL protocol are prone to attack or roll back. Do not set this parameter with "Any".
			
			Remediation:
			`SSL_VERSION = 3.0`
			
			Audit:
			`grep –i SSL_VERSION sqlnet.ora`
				√	√	2
						S

5.16	OAS – SSL Cipher Suite	Set SSL Cipher Suite.
		`SSL_CIPHER_SUITES = SSL_RSA_WITH_3DES_EDE_CBC_SHA)`
			Rationale:
			SSL_CIPHER_SUITES are automatically set to FIPS140-2 approved suites by Oracle 11g. The following is for reference.
			
			Remediation:
			`SSL_CIPHER_SUITES =(`
			`SSL_DH_anon_WITH_3DES_EDE_CBC_SHA,`
			`SSL_DH_anon_WITH_DES_CBC_SHA,`
			`SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA,`
			`SSL_RSA_WITH_3DES_EDE_CBC_SHA,`
			`SSL_RSA_WITH_DES_CBC_SHA,`
			`SSL_RSA_EXPORT_WITH_DES40_CBC_SHA)`
			
			Audit:
			`grep –i SSL_CIPHER_SUITES sqlnet.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

5.17	OAS – SSL Client DN Match	Set `tnsnames` file to include `SSL_SERVER_CERT_DN` parameter with the distinguished name (DN) of the certificate.	**Rationale:**
			This will reduce the possibility of certificate masquerading which can lead to man in the middle attacks and compromise the security provided by the SSL protocol.
			
			Remediation:
			`SSL_SERVER_CERT_DN= \`
			`"cn=dept,cn=OracleContext,dc=us,dc=acme,\`
			`dc=com"`
			
			Audit:
			`grep –i SSL_SERVER_CERT_DN tnsnames.ora`
				√	√	2
						S

5.18	OAS – SSL Client Authentication	`SSL_CLIENT_`
		`AUTHENTICATION=TRUE`
			Rationale:
			It is preferable to have mutually authenticated SSL connections verifying the identity of both parties. If possible use client and server certificates for SSL connections. If client certificates are not supported in the enterprise, then set to `FALSE`.
			
			Remediation:
			`SSL_CLIENT_AUTHENTICATION=true`
			
			Audit:
			`grep –i SSL_CLIENT_AUTHENTICATION \`
			`sqlnet.ora`
				√	√	2
						S

5.19	OAS – Encryption Tab	Use OAS encryption only if SSL is not feasible.	**Rationale:** OAS Integrity/Encryption should only be used if required because of non-SSL clients. **Remediation:** None **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.20	Encryption	Where possible, use a procedure that employs a content data element as the encryption key that is unique for each record.	**Rationale:** 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. **Remediation:** None **Audit:** None	√	√	2 N
5.21	Encryption	Use RAW or BLOB for the storage of encrypted data.	**Rationale:** 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. **Remediation:** None **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.22	Encryption	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. The column name should be obscure and should not reveal the role of the column. Rows should be protected with both VPD and OLS (OLS included VPD) and the keys themselves should be encrypted with a master key. If the keys are managed by an application or generated as computed keys the procedures should be wrapped. All package bodies, procedures, and functions should be wrapped.	**Rationale:** 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. **Remediation:** Use multiple layers of protection when storing keys with the data in a separate database. Employ wrapping to protect all code used to protect, generate keys for, or encrypt keys. If security dictates, hardware devices can be used for encryption key storage. Keys, at minimum, should follow password selection standards in areas of minimum length, use of special characters and non-dictionary words. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

5.23	Encryption	Revoke the `PUBLIC` execute privileges from the `DBMS_OBFUSCATION_TOOLKIT` .	**Rationale:**
			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 available 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 available for malicious use.
			
			Remediation:
			`REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT TO PUBLIC;`
			
			Audit:
			`SELECT TABLE_NAME FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_OBFUSCATION_TOOLKIT';`
				√	√	2
						S

5.24	Encryption	Use HSM for storage of master key.	**Rationale:** Where possible use an HSM to store the master keys for Transparent Data Encryption. All encryption and decryption operations that use the master encryption key are performed inside the HSM. This means that the master encryption key is never exposed in insecure memory. **Remediation:** None **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
5.25	Encryption	Tablespace Encryption	**Rationale:** When a table contains a large number of columns of PII it can be beneficial to encrypt an entire tablespace rather than columns. **Remediation:** Use tablespace encryption . **Audit:** None	√	√	2 N

5.26	Radiuskey	Verify and set permissions on `radius.key` file	**Rationale:**
			File permissions must be restricted to the owner of the Oracle software and `dba` group. Ensure proper permissions are set on `$ORACLE_HOME/network/security/radius.key`
			
			Remediation:
			`chmod 440 \`
			`$ORACLE_HOME/network/security/radius.key`
			
			Audit:
			`ls -al \`
			`$ORACLE_HOME/network/security/radius.key`
				√	√	1
						S

5.27	sqlnet.ora	`SSL_CERT_REVOCATION=required`	**Rationale:**
			Ensure revocation is required for checking CRLs for client certificate authentication. Revoked certificates can pose a threat to the integrity of the SSL channel and should not be trusted.
			
			Remediation:
			`SSL_CERT_REVOCATION=required`
			
			Audit:
			`grep -i SSL_CERT_REVOCATION sqlnet.ora`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

5.28	sqlnet.ora	`SSL_SERVER_DN_MATCH=yes`	**Rationale:**
			Ensure the DN string of the certificate matches the expected value.
			
			Remediation:
			`SSL_SERVER_DN_MATCH=yes`
			
			Audit:
			`grep -i SSL_SERVER_DN_MATCH sqlnet.ora`
				√	√	2
						S

6. Startup and Shutdown

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

6.01	Advanced queuing in asynchronous messaging	Empty queue at shut down of Oracle.	**Rationale:**
			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.
			
			Remediation:
			Empty queues at the shutdown of the Oracle instances.
			`DBMS_AQADM.PURGE_QUEUE_TABLE(`
			`queue_table => 'name.obj_qtab',`
			`purge_condition => NULL,`
			`purge_options => po);`
			
			`DBMS_AQADM.PURGE_QUEUE_TABLE(`
			`queue_table => 'bane.obj_qtab',`
			`purge_condition => 'qtview.queue = ''NAME.OBJ_QUEUE''',`
			`purge_options => po);`
			
			Audit:
			None
				√	√	1
						N

6.02	Cache	Cache must be emptied at shut down of Oracle.	**Rationale:** Information in caches may be accessed outside of Oracle and beyond the controls of the security parameters. **Remediation:** `ALTER SYSTEM FLUSH BUFFER_CACHE;` **Audit:** None	√	√	1 N

7. Backup and Disaster Recovery

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
7.01	Redo logs	Mirror	**Rationale:** Redundancy for the redo logs can prevent catastrophic loss in the event of a disk or system failure. **Remediation:** Mirror on-line redo logs and ensure that more than one group exists. **Audit:** None	√	√	1 N
7.02	Control files	Multiplex control files to multiple physical disks.	**Rationale:** Redundancy for the control files can prevent catastrophic loss in the event of a single physical drive failure **Remediation:** Store control files on a RAID or other redundant disk system. **Audit:** None .	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
7.03	Control files	Mirror	**Rationale:** Mirror the Oracle control files. In the event that the control files become corrupted or a system failure mirroring will help ensure recovery is possible. **Remediation:** Mirror control files to multiple separate physical partitions. **Audit:** None	√	√	1 N
7.04	Archive logs	Ensure there is sufficient space for the archive logging process.	**Rationale:** Without adequate space for the archive logs the system will hang resulting in a denial of service. **Remediation:** Allocate more disk space to redo log partitions. **Audit:** None	√	√	1 N
7.05	Redo logs	Multiplex redo logs to multiple physical disks.	**Rationale:** Redundancy for the redo logs can prevent catastrophic loss in the event of a single physical drive failure. **Remediation:** None **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
7.06	Archive log files	Backup	**Rationale:** Archived logs contain sensitive information and must be properly handled. **Remediation:** If archive log 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. **Audit:** None	√	√	1 N
7.07	Backup	Automated backups should be verified.	**Rationale:** 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. **Remediation:** 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. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
7.08	Failsafe	Failsafe must be engaged.	**Rationale:** Failsafe uses the cluster server interface to provide the failover protection previously provided by hardware interfaces. **Remediation:** Engage failsafe. **Audit:** None	√		2 N

8. Oracle Profile (User) Setup Settings

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.01	Database Profiles	`failed_login_attempts=3`	**Rationale:**
			Restricting the number of login attempts will help deter brute force attacks against profiles.
			
			Remediation:
			Application accounts must be set for `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.
			
			Create a profile then assign it to a user account. Default profile has this setting at 10.
			
			`ALTER PROFILE profile_name LIMIT FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME 1;`
			
			Note: It is recommended to create three separate profiles: Application accounts, system accounts, and user accounts instead of using the default for all.
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS'`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.02	Database Profiles	`password_life_time= 90`	**Rationale:**
			Restricting the password lifetime will help deter brute force attacks against user accounts and refresh passwords.
			
			Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.
			Create a profile then assign it to a user account.
			Default profile has a setting of 180
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT password_life_time 90;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_LIFE_TIME'`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.03	Database Profiles	`password_reuse_max=20`	**Rationale:**
			`password_reuse_max` sets the number of different passwords that must be rotated by the user before the current password can be reused. This prevents users from cycling through a few common passwords and helps ensure the integrity and strength of user credentials.
			
			Local policy may override the recommended setting. This setting may not be applicable for middle tier application accounts that access the database.
			
			Create a profile then assign it to a user account. Default profile has a setting of `UNLIMITED`.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT password_reuse_max 20;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_REUSE_MAX'`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.04	Database Profiles	`password_reuse_time= 365`	**Rationale:**
			`password_reuse_time` sets the amount of time that must pass before a password can be reused. Creating a long window before password reuse helps protect from password brute force attacks and helps the strength and integrity of the user credential.
			
			Local policy may not override the setting. Create a profile then assign it to a user account. Default profile has this setting as `UNLIMITED`
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT password_reuse_time 365;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_REUSE_TIME'`
				√	√	1
						S

8.05	Database Profiles	`password_lock_time=1`	**Rationale:**
			`password_lock_time` specifies the amount of time in days that the account will be locked out if the maximum number of authentication attempts has been reached.
			
			Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT password_lock_time 1;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_LOCK_TIME'`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.06	Database Profiles	`password_grace_time=3`	**Rationale:**
			`password_grace_time` specified in days the amount of time that the user is warned to change their password before their password expires.
			
			Local policy may not override the setting. This setting may not be applicable for middle tier application accounts that access the database.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT password_grace_time 3;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_GRACE_TIME'`
				√	√	1
						S

8.07	Database Profiles	Review accounts where `PASSWORD= 'EXTERNAL'`	**Rationale:**
			Check and review any user who has `password='EXTERNAL'`. Do not allow remote OS authentication to the database.
			
			Remediation:
			`ALTER USER <username> IDENTIFIED BY <new_password>;`
			
			Audit:
			`SELECT USERNAME FROM DBA_USERS WHERE PASSWORD='EXTERNAL';`
				√	√	2
						N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.08	Database Profiles	Set `password_verify_function` to a verification function	**Rationale:**
			Allow `password_verification_function` to be called when passwords are changed. This always works for password changes via the "password" command at an SQL prompt.
			
			Remediation:
			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:
			
			`PASSWORD_GRACE_TIME 3`
			`PASSWORD_REUSE_TIME 365`
			`PASSWORD_REUSE_MAX 20`
			`FAILED_LOGIN_ATTEMPTS 3`
			`PASSWORD_LOCK_TIME 1`
			
			Modify the line:
			`IF length(password) < 4`
			by changing the minimum password length to 8.
			Do not use the `verify_function_11G` as it sets password settings to the defaults listed above.
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_VERIFY_FUNCTION';`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.09	Database Profiles	Set `CPU_PER_SESSION` as appropriate	**Rationale:**
			Allowing a single application or user to consume excessive CPU resources will result in a denial of service to the Oracle database. Ensure that users profile settings have appropriate values set for the particular database and application.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT CPU_PER_SESSION <value>;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='CPU_PER_SESSION';`
				√	√	2
						S

8.10	Database Profiles	Set `PRIVATE_SGA` as appropriate	**Rationale:**
			Allowing a single application or user to consume the excessive amounts of the System Global Area will result in a denial of service to the Oracle database. Ensure that users profile settings have appropriate values set for the particular database and application.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT PRIVATE_SGA <value>;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' PRIVATE_SGA';`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
8.11	Database Profiles	Set LOGICAL_READS_ PER_SESSION as appropriate	**Rationale:** Allowing a single application or user to perform excessive amounts of reads to disk will result in a denial of service to the Oracle database. Ensure that users profile settings have appropriate values set for the particular database and application. **Remediation:** ALTER PROFILE profile_name LIMIT LOGICAL_READS_ PER_SESSION <value>; **Audit:** SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' LOGICAL_READS_PER_SESSION';	√	√	2 S
8.12	Database Profiles	Set SESSIONS_PER_USER as appropriate	**Rationale:** Allowing an unlimited amount of sessions per user can consume Oracle resources and cause a denial of service. Limit the number of session for each individual user. Ensure that users profile settings have appropriate values set for the particular database and application. **Remediation:** ALTER PROFILE profile_name LIMIT SESSIONS_PER_USER <value>; **Audit:** SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' SESSIONS_PER_USER';	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
8.13	Database Profiles	Set CONNECT_TIME as appropriate	**Rationale:** Sessions held open for excessive periods of time can consume system resources and cause a denial of service for other users of the Oracle database. The CONNECT_TIME parameter limits the upper bound on how long a session can be held open. This parameter is specified in minutes. Sessions that have exceeded their connect time are aborted and rolled back. Note: Oracle does not do strict monitoring of connect times and sessions can exceed this time limit by up to a few minutes. Ensure that users profile settings have appropriate values set for the particular database and application. **Remediation:** ALTER PROFILE profile_name LIMIT CONNECT_TIME <value>; **Audit:** SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' CONNECT_TIME';	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

8.14	Database Profiles	Set `IDLE_TIME` as appropriate	**Rationale:**
			Idle sessions held open for excessive periods of time can consume system resources and cause a denial of service for other users of the Oracle database. Limit the maximum number of minutes a session can idle. Ensure that users profile settings have appropriate values set for the particular database and application.
			
			Remediation:
			`ALTER PROFILE profile_name LIMIT IDLE_TIME <value>;`
			
			Audit:
			`SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' IDLE_TIME';`
				√	√	2
						N

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 and DBA have most of these accesses and privileges, and should be the only users granted permissions.

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.01	Tablespaces	Do not have `default_tablespace` set to `SYSTEM` for user accounts	**Rationale:**
			Only SYS should have a default tablespace of `SYSTEM`. This prevents administrative users from altering system objects. Note it may be difficult or impossible to move some objects.
			
			Remediation:
			`ALTER USER DEFAULT_TABLESPACE table;`
			
			Audit:
			`SELECT USERNAME, DEFAULT_TABLESPACE FROM DBA_USERS;`
				√	√	2
						S

9.02	Tablespaces	Ensure application users have not been granted quotas on tablespaces.	**Rationale:**
			Set quotas for developers on shared production/development systems to prevent space resource contentions. Application users should be granted quotas on a case by case basis to avoid application failure.
			
			Remediation:
			`ALTER USER <USER_NAME> QUOTA <VALUE> ON <TABLESPACE_NAME>;`
			
			Audit:
			`SELECT <USERNAME> FROM DBA_TS_QUOTAS WHERE USERNAME='USER' AND TABLESPACE_NAME='TABLESPACE_NAME';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.03	Any dictionary object	Review access and revoke access where possible	**Rationale:** Check for any user that has access to any dictionary object and revoke where possible. This reduces the overall privileges of the user base and reduces the attack surface of the Oracle database. **Remediation:** Review access rights and revoke privileges where possible. **Audit:** None	√	√	1 N

9.04	Tables	Prevent access to `SYS.AUD$`	**Rationale:**
			Check for any user accounts that have access and revoke where possible. This is only applicable if the audit trail parameter is set to `db` or `db_extended`. Allowing users to alter the `AUD$` table can compromise the audit trail or integrity of the Oracle database.
			
			Remediation:
			`REVOKE ALL ON SYS.AUD$ FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='AUD$'`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.05	Tables	Prevent access to SYS.USER_HISTORY$	**Rationale:** Revoke access to this table from all users and roles except for SYS and DBA accounts. Allowing users to alter the USER_HISTORY$ table can compromise the audit trail or integrity of the Oracle database. **Remediation:** REVOKE ALL ON SYS.USER_HISTROY$ FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER_HISTORY$';	√	√	1 S
9.06	Tables	Prevent access to SYS.LINK$	**Rationale:** Sensitive user and password data is stored in the LINK$ table. Non administrative or system users should be prevented from accessing this table. Check for any user that has access and revoke where possible. **Remediation:** REVOKE ALL ON SYS.LINK$ FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='LINK$';	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.07	Tables	Prevent access to SYS.USER$	**Rationale:** Sensitive user and password data is stored in the USER$ table. Only administrative or system users should have rights to access this table. Check for any user that has access and revoke where possible. **Remediation:** REVOKE ALL ON SYS.USER$ FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER$';	√	√	1 S
9.08	Tables	Prevent access to SYS.SOURCE$	**Rationale:** Allowing users to alter codes in the SOURCE$ table can compromise the security and integrity of the Oracle database. Check for any user accounts that have access and revoke where possible. **Remediation:** REVOKE ALL ON SYS.SOURCE$ FROM <USER> ; **Audit:** SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WERE TABLE_NAME='SOURCE$';	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.09	Tables	Prevent access to PERFSTAT.STATS$SQLTEXT	**Rationale:** Check for any user that has access and revoke where possible. SQLTEXT stores the full text of SQL statements that have been executed and can contain sensitive information. **Remediation:** REVOKE ALL ON PERFSTAT.STATS$SQLTEXT; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='STATS$SQLTEXT';	√	√	1 S
9.10	Tables	Prevent access to PERFSTAT.STATS$SQL_SUMMARY	**Rationale:** Check for any user that has access and revoke where possible. SQL_SUMMARY contains the first few lines of the executed SQL statements and can contain sensitive information. **Remediation:** REVOKE ALL ON PERFSTAT.STATS$SQLSUM; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='STATS$SQLSUM';	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.11	Tables	Prevent access to any `X$` table	**Rationale:**
			`X$` tables are kernel tables used by Oracle internals and should not be accessed by users. Check for any user that has access and revoke where possible.
			
			Remediation:
			`REVOKE ALL ON X$<TABLENAME> FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE('X$%');`
				√	√	1
						S

9.12	Views	Prevent access to any `DBA_` views	**Rationale:**
			`DBA` views return information about all objects and should only be accessible by administrators. Check for any user that has access and revoke where possible.
			
			Remediation:
			`REVOKE ALL ON DBA_<TABLENAME> FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE('DBA_$%');`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.13	Views	Prevent access to any V$ views	**Rationale:** V$ tables contain sensitive information about Oracle database and should only be accessible by system administrators. Check for any user that has access and revoke where possible. **Remediation:** REVOKE ALL ON TABLE_NAME FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE('V$%');	√	√	1 S
9.14	Views	Prevent access to ALL_SOURCE	**Rationale:** ALL_SOURCE contains the text source for all of the user's objects. Check for any user that has access and revoke where possible. **Remediation:** REVOKE ALL ON ALL_ SOURCE FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='ALL_SOURCE';	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.15	Views	Prevent access to DBA_ROLES	**Rationale:** Allowing the user to alter the DBA_ROLES can result in privilege escalation or system instability. Restrict access to this view to all users except SYS and DBAs. **Remediation:** REVOKE ALL ON DBA _ROLES FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=DBA_ROLES’;	√	√	1 S
9.16	Views	Prevent access to DBA_SYS_PRIVS	**Rationale:** Allowing a user to access the dba_sys_privs table will show the users’ privileges for all users in the Oracle database. Restrict access to this view to all users except SYS and DBAs. **Remediation:** REVOKE ALL ON DBA_SYS_PRIVS FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=DBA_SYS_PRIVS’;	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.17	Views	Prevent access to DBA_ROLE_PRIVS	**Rationale:** Allowing a user to access the dba_role_privs view will show the role privileges for all roles in the Oracle database. Restrict access to this view to all users except SYS and DBAs. **Remediation:** REVOKE ALL ON DBA_ROLE_PRIVS FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=DBA_ROLE_PRIVS’;	√	√	1 S
9.18	Views	Prevent access to DBA_TAB_PRIVS	**Rationale:** Allowing a user to access the dba_tab_privs view will show the table privileges for all users in the Oracle database. Restrict access to this view to all users except SYS and DBAs. **Remediation:** REVOKE ALL ON DBA_TAB_PRIVS FROM <USER>; **Audit:** SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=DBA_ TAB _PRIVS’;	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.19	Views	Prevent access to `DBA_USERS`	**Rationale:**
			Allowing a user to access the `dba_users` view will show the role privileges for all users in the Oracle database. Restrict access to this view to all users except SYS and DBAs.
			
			Remediation:
			`REVOKE ALL ON DBA_USERS FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=DBA_USERS';`
				√	√	1
						S

9.20	Views	Prevent access to `ROLE_ROLE_PRIVS`	**Rationale:**
			Allowing a user to access the `dba_role_privs` view will show the role grants for all roles in the Oracle database. Restrict access to this view to all users except SYS and DBAs.
			
			Remediation:
			`REVOKE ALL ON ROLE_ROLE_PRIVS FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=' ROLE_ROLE_PRIVS;`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.21	Views	Prevent access to `USER_TAB_PRIVS`	**Rationale:**
			Allowing a user to access the `user_tab_privs` view will show the granted table privileges for all users in the Oracle database. Restrict access to this view to all users except SYS and DBAs.
			
			Remediation:
			`REVOKE ALL ON USER_TAB_PRIVS FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER_TAB_PRIVS;`
				√	√	1 S

9.22	Views	Prevent access to `USER_ROLE_PRIVS`	**Rationale:**
			Allowing a user to access the `user_role_privs` view will show the granted role privileges for all users in the Oracle database. Restrict access to this view to all users except SYS and DBAs.
			
			Remediation:
			`REVOKE ALL ON USER_ROLE_PRIVS TO <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=' USER_ROLE_PRIVS;`
				√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.23	Roles	Prevent assignment of roles that have `_CATALOG_`	**Rationale:**
			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`.
			
			Remediation:
			`REVOKE ALL ON <ROLE> FROM <USER>;`
			
			Audit:
			`SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE('%_CATALOG_%');`
				√	√	1
						S

9.24	Synonyms	Prevent access to any `V$` synonym	**Rationale:** Check for any user that has access and revoke where possible. **Remediation:** Delete the synonym or revoke the privileges **Audit:** `SELECT SYNONYM_NAME, TABLE_NAME FROM ALL_SYNONYMS WHERE TABLE_NAME LIKE('V$%');`	√	√	1 S
9.25	Synonyms	When dropping synonyms, ensure privileges granted to the synonyms, if not required, are removed from the base objects.	**Rationale:** Granting privileges to synonyms actually grants privileges to the base objects. **Remediation:** If necessary, ensure that privileges from the base objects are removed when the synonyms are dropped. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.26	Privileges	Restrict system privileges	**Rationale:**
			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.
			
			Remediation:
			`REVOKE ALL <PRIVS> FROM <USER>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS;`
				√	√	1
						S

9.27	Privileges	Prevent granting of privileges that contain the keyword `ANY`	**Rationale:** The `ANY` keyword grants the ability for the user to set privileges for the entire catalogue of objects in the database. **Remediation:** Check for any user or role that has the `ANY` keyword and revoke this role where possible. **Audit:** `SELECT * FROM DBA_SYS_PRIVILEGES WHERE PRIVILEGE LIKE('%ANY%');`	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.28	Privileges	Prevent granting of all privileges	**Rationale:**
			The `GRANT ALL PRIVILEGES` must not be used; it gives full access to all tables, views and objects to the user or role it is granted to.
			
			Remediation:
			`REVOKE ALL PRIVILEGES FROM <USER/ROLE>`
			`GRANT <SPECIFIC PRIVILEGES> TO <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT ANY PRIVILEGE';`
			
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT ANY OBJECT PRIVILEGE';`
				√	√	2
						N

9.29	Privileges	Prevent granting of `EXEMPT ACCESS POLICY` (EAP)	**Rationale:**
			Revoke this privilege if not necessary.
			The EAP privilege provides access to all rows regardless of Row Level Security assigned to specific rows.
			
			Remediation:
			`REVOKE EXEMPT ACCESS POLICY FROM <USER>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXEMPT ACCESS POLICY';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.30	Privileges	Prevent granting of privileges that have `WITH ADMIN`	**Rationale:**
			Check for any user or role that has been granted privileges `WITH ADMIN` and revoke where possible. The `WITH ADMIN` privilege allows a user to grant the same privileges they possess.
			
			Remediation:
			`REVOKE <ROLE> FROM <USER>;`
			`GRANT <ROLE> TO <USER>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE ADMIN_OPTION=”YES”;`
				√	√	1
						S

9.31	Privileges	Prevent granting of privileges that have `WITH GRANT`	**Rationale:**
			Check for any user or role that has been granted privileges `WITH GRANT` and revoke where possible. The `WITH GRANT` privilege allows a user to grant the same privilege to other users.
			
			Remediation:
			`REVOKE GRANT OPTION FOR <PRIV> ON <TABLE> FROM <USER>;`
			
			Audit:
			`SELECT * FROM DBA_TAB_PRIVS WHERE GRANTABLE='YES';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.32	Privileges	Prevent granting of privileges that have `CREATE`	**Rationale:**
			Check for any user that has object creation privileges and revoke where possible. Excessive create privileges can allow an attack to create arbitrary objects, tables, and views.
			
			Remediation:
			`REVOKE CREATE <PRIV> FROM <USER/ROLE>`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIV FROM PRIVILEGE LIKE('CREATE %');`
				√	√	1
						S

9.33	Privileges	Prevent granting of `CREATE LIBRARY`	**Rationale:**
			Check for any user or role that has this privilege and revoke where possible. The `CREATE LIBRARY` privilege allows a user to create an object associated with a shared library. Allowing arbitrary library creation can compromise the integrity and security of the Oracle database.
			
			Remediation:
			`REVOKE CREATE LIBRARY FROM <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE LIBRARY';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.34	Privileges	Prevent granting of `ALTER SYSTEM`	**Rationale:**
			Check for any user or role that has this privilege and revoke where possible. The alter system privilege allows a user to dynamically alter the Oracle instance.
			
			Remediation:
			`REVOKE ALTER SYSTEM FROM <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='ALTER SYSTEM';`
				√	√	1
						S

9.35	Privileges	Prevent granting of `CREATE PROCEDURE`	**Rationale:**
			`CREATE PROCEDURE` allows a user to create a stored procedure in the database and should be restricted to administrative or development users. Check for any user or role that has this privilege and revoke where possible.
			
			Remediation:
			`REVOKE CREATE PROCEDURE FROM <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE PROCEDURE';`
				√	√	1
						S

9.36	Privileges	Prevent granting of `BECOME USER`	**Rationale:**
			`BECOME USER` allows a user to inherit the rights of another oracle system user and should not be used if possible.
			
			Remediation:
			`REVOKE BECOME USER FROM <USER/ROLE>`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE('BECOME USER');`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.37	Privileges	Prevent granting of `SELECT ANY TABLE`	**Rationale:**
			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.
			
			Remediation:
			`REVOKE SELECT ANY <OBJECT> FROM <USER>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE('SELECT ANY%');`
				√	√	1
						S

9.38	Privileges	Prevent granting of `AUDIT SYSTEM`	**Rationale:**
			Review which users have audit system privileges and limit as much as possible to ensure audit commands are not revoked.
			
			Remediation:
			`REVOKE <PRITILEGE> FROM <USER>;`
			
			Audit:
			`SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='AUDIT SYSTEM';`
				√	√	1
						S

9.39	Privileges	Grant privileges only to roles	**Rationale:** Grant privileges only to roles. Do not grant privileges to individual users. **Remediation:** Revoke all individual privileges from users. Create a role defining the needed privileges. Grant the role to the users. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.40	Privileges	Review privileges granted to `PUBLIC`	**Rationale:**
			Review all privileges granted to `PUBLIC`. Limit or revoke unnecessary `PUBLIC` privileges.
			
			Remediation:
			`REVOKE PUBLIC FROM <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='PUBLIC';`
				√	√	1
						S

9.41	Roles	Prevent assignment of `RESOURCE`	**Rationale:**
			Revoke the resource role from normal application user accounts.
			
			Remediation:
			`REVOKE RESOURCE FROM <USER/ROLE>;`
			
			Audit:
			`SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='RESOURCE';`
				√	√	1
						S

9.42	Roles	Prevent assignment of `DBA`	**Rationale:**
			Assigning the DBA role to users provides unnecessary access and control of the Oracle database.
			
			Remediation:
			Revoke DBA role from users who do not require it.
			`REVOKE DBA FROM <USER/ROLE>`
			
			Audit:
			`SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.43	Packages	ACL or Deny access to `UTL_FILE`	**Rationale:**
			Review the ACL for usage of the `UTL_FILE` package. Revoke the public execute privilege on `UTL_FILE` as it can be used to access O/S.
			
			Remediation:
			`REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='UTL_FILE';`
				√	√	1
						S

9.44	Packages	ACL or Deny access to `UTL_TCP`	**Rationale:**
			Review the ACL for usage of the `UTL_TCP` package. Revoke the public execute privilege on `UTL_TCP` as it can write and read sockets.
			
			Remediation:
			`REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='UTL_TCP';`
				√	√	1
						S

9.45	Packages	ACL or Deny access to `UTL_HTTP`	**Rationale:**
			Review the ACL for usage of the `UTL_HTTP` package. Revoke the public execute privilege on `UTL_HTTP` as it can write content to a web browser.
			
			Remediation:
			`REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='UTL_HTTP';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.46	Packages	ACL or Deny access to `UTL_SMTP`	**Rationale:**
			Review the ACL for usage of the `UTL_SMTP` packageRevoke the public execute privilege on `UTL_SMTP` as it can send mail from the database server.
			
			Remediation:
			`REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='UTL_SMTP';`
				√	√	1
						S

9.47	Packages	Deny access to `DBMS_LOB`	**Rationale**
			Revoke the public execute privilege. This procedure allows the manipulation of large objects and BFILE file read access. If not required its usage should be revoked.
			
			Remediation:
			`REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_LOB';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.48	Packages	Deny access to `DBMS_SYS_SQL`	**Rationale**
			Revoke the public execute privilege. If public permissions are granted on DBMS_SYS_SQL a user can acquire an administrative cursor and act with DBA permissions.
			
			Remediation:
			`REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_SYS_SQL';`
				√	√	1
						S

9.49	Packages	Deny access to `DBMS_JOB`	**Rationale**
			Revoke the public execute privilege. DBMS_JOB is a backwards compatible job scheduler for Oracle. If no longer required its usage should be disabled to reduce Oracle's attack surface.
			
			Remediation:
			`REVOKE EXECUTE ON DBMS_JOB TO PUBLIC;`
			
			Audit:
			`SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_JOB';`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.50	Proxy Authentication	Limit the user schema privileges to `CREATE SESSION` only.	**Rationale**
			The proxy account should only have the ability to connect to the database. No other privileges should be granted to this account.
			
			Remediation:
			`REVOKE ALL ON <USER>;`
			`GRANT CREATE SESSION TO <USER>;`
			
			Audit:
			`SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE='<PROXY ACCOUNT>';`
			`SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE='<PROXY ACCOUNT>';`
			`SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE='<PROXY ACCOUNT>';`
				√	√	1
						S

9.51	Proxy role	Restrict the roles that can be enabled when privileges are granted in the database.	**Rationale**
			If application roles have been granted to user then these roles need to be prevented from being enabled by default on the subsequent logins.
			
			Remediation:
			`CREATE ROLE 'X' ;`
			`GRANT 'X' TO JOHN_SMITH;`
			`ALTER USER JOHN_SMITH DEFAULT ROLE ALL EXCEPT X;`
			
			Audit:
			None
				√	√	1
						N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.52	Views	Revoke public access to all public views that start with `ALL_`	**Rationale**
			Revoke access to these views when possible to prevent unauthorized access to data that could be sensitive.
			
			Note: This may interfere with some applications.
			
			Remediation:
			`REVOKE ALL ON ALL_<NAME> FROM PUBLIC;`
			
			Audit:
			`SELECT TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE('ALL_%') AND GRANTEE='PUBLIC';`
				√	√	2
						S

9.53	Roles and Privileges	When dropping a user, ensure roles and privileges created by that user, if not required, are deleted.	**Rationale** Dropping a user (i.e., `DROP USER X CASCADE`) doesn't delete roles and privileges created by the user. **Remediation:** If a user is dropped, ensure that the roles and privileges created by that user, if not required, are deleted. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
9.54	Packages	Limit or deny access to DBMS_BACKUP_RESTORE	**Rationale** Provides file system functions such as copying files, altering control files, accessing devices, and deleting files. **Remediation:** REVOKE EXECUTE ON DBMS_BACKUP_RESTORE TO PUBLIC; REVOKE EXECUTE ON DBMS_BACKUP_RESTORE TO <USER>; **Audit:** SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_BACKUP_RESTORE';	√	√	R
9.55	Packages	Audit usage of DBMS_RANDOM	**Rationale** Audit the DBMS_RANDOM function in applications for improper usage. DBMS_RANDOM should not be used for critical functions related to cryptography, session id generation or other areas where a high degree of entropy is required. Replace calls to these functions with RANDOMBYTES, Revoking the public privilege may cause some applications to fail it is suggested that if the public execute permission cannot be revoked the applications that utilize DBMS_RANDOM are carefully audited. **Remediation:** REVOKE EXECUTE ON DBMS_RANDOM TO PUBLIC; **Audit:** SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_RANDOM';	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

9.56	Roles	Password protect roles	**Rationale**
			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.
			
			Remediation:
			`SET ROLE <ROLE_NAME> IDENTIFIED BY <ROLE_PASSWORD>;`
			
			Audit:
			`SELECT * FROM DBA_ROLES;`
				√	√	2
						S

10. Enterprise Manager / Grid Control / Agents

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
10.01	Enterprise Management studio mode	Access to the enterprise management in studio must be limited.	**Rationale:** Without limitations on the enterprise management access to the remote agents is virtually unlimited. **Remediation:** Limit access to the Oracle Enterprise Management studio. **Audit:** None	√	√	1 N
10.02	Enterprise Manager Agent File uploads	Monitor the size of file uploads from the enterprise agent.	**Rationale:** The following lines are some of the output from the `./emctl` status agent command containing information regarding the agents uploading files: Total Megabytes of XML files uploaded so far : Number of XML files pending upload: Size of XML files pending upload(MB): Discovering unusual or increased size of file uploads could indicate a malicious agent. **Remediation:** Create a monitor to track the size of file uploads from the enterprise agent. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
10.03	Enterprise Manager Framework Security	Where possible, utilize Enterprise Manager Framework Security Functionality.	**Rationale:** Enterprise Manager Framework security employs secure communication between the various Enterprise Manager Components, i.e., **Remediation:** Enable HTTPS between management agents and management services. **Audit:** None	√	√	1 N

10.04	Grid Control TimeOut Value	Configure an appropriate value for Grid Control Timeout value in the Oracle Application Server.
		
		File:
		`$IAS_HOME/sysman/config/emoms.properties`
		
		Value:
		`oracle.sysman.eml.maxInactiveTime=time_in_minutes`
			Rationale:
			To prevent unauthorized access to the Grid Control via browser, set an appropriate timeout value. A value of 30 minutes or less is recommended. The default is 45 minutes.
			
			Remediation:
			Edit the `$IAS_HOME/sysman/config/emoms.properties` file and set the value to 30
			
			Audit:
			`grep –i maxInactiveTime \ $IAS_HOME/sysman/config/emoms.properties`
				√	√	1
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
10.05	Enterprise Manager Framework Security	In command line mode, avoid using commands that contain passwords in the arguments.	**Rationale:** While registering an agent to utilize the enterprise manager framework security, avoid using sensitive command line arguments for `emctl`. The command can be captured by other users with access to Unix (via `ps`) command or can be prone to shoulder surfing. Some Unix shells, like bash, log command history as well. This may be another exposure. **Remediation:** In command line mode, avoid using commands that contain passwords in the arguments. **Audit:** None	√	√	1 N
10.06	Oracle Installation	Separate user account for Management/Intelligent Agent	**Rationale:** The agent database accounts must be separated. This will isolate the Agent from the rest of the Oracle server in the event that is compromised. **Remediation:** For Unix systems, create a unique user account for the management/Intelligent Agent process in order to differentiate accountability and file access controls. Separate accounts are not recommended for Windows environments. **Audit:** None		√	2 N

11. Specific Systems

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
11.01	ADDM	Verify ADDM suggestions	**Rationale:** Automatic Database Diagnostic Monitor (ADDM), should not blindly replace the DBA's knowledge. **Remediation:** DBA's should verify the applicability of ADDM suggestions based on their knowledge of the database. **Audit:** None	√	√	1 N
11.02	AMM	Monitor AMM	**Rationale:** Automated Memory Manager (AMM), should not blindly replace the DBA's knowledge. **Remediation:** DBA's should monitor AMM to ensure memory is being properly allocated. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
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.	**Rationale:** 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 available 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. **Remediation:** Implement AWR to record all database performance statistics (related to object usage, SQL statement efficiency, session history, etc) over a defined time period. **Audit:** None	√	√	1 N
11.04	Fine grained access	Use fine grain access control within objects.	**Rationale:** 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. **Remediation:** Evaluate sensitive areas of the Oracle database and enable fine grain access control . **Audit:** None	√	√	2 N

12. General Policy and Procedures

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.00	Oracle Installation	Do not install Oracle on an Internet facing server.	**Rationale:** Oracle must only be installed on a backend system behind appropriate firewalling or other network protection systems. **Remediation:** Do not install Oracle on an Internet facing server migrate internet facing oracle servers to a backend or protected environment. **Audit:** None	√	√	1 N
12.01	Oracle alert log file	Review contents	**Rationale:** The Oracle alert log file must be regularly reviewed for errors. Periodically review logs for errors, large numbers or exotic errors can be an indicator of a system under attack. **Remediation:** Assign an administrator or DBA to review the log files. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.02	Database creation scripts on host	Remove or secure	**Rationale:** System creation scripts can provide an attacker with valuable information about the Oracle setup or instance and often contain errors. **Remediation:** Delete the scripts from the database host. After the database has been created, remove the scripts or at a minimum move them to a safe repository area. **Audit:** None	√	√	1 N
12.03	Unix root group members on host	Disallow 'oracle' as member of root group	**Rationale:** The Oracle software owner account must not be a member of the root group on Unix systems. Having the Oracle account part of the root group breaks privilege separation and best security practices. **Remediation:** Edit `/etc/group` remove the `oracle_account` from the root group **Audit:** `grep oracle_account /etc/group`		√	1 N
12.04	Oracle DBA group membership on host	Review	**Rationale:** 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. **Remediation:** Remove unnecessary users from the `DBA` group. **Audit:** `cat /etc/group`	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.05	Sensitive information in process list on host	Avoid or encrypt	**Rationale:** Revealing username and password information in the process list will give anyone able to perform a process listing a valid set of user credentials for the Oracle database. **Remediation:** 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. **Audit:** None	√	√	1 N
12.06	Sensitive information in cron jobs on host	Avoid or encrypt	**Rationale:** 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. **Remediation:** Encrypt passwords used in `cron` on batch jobs. **Audit:** None		√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.07	Sensitive information in at jobs (or jobs in Windows scheduler) on host	Avoid or encrypt	**Rationale:** An enforced policy must exist to ensure that no at jobs (or jobs in Windows scheduler) have sensitive information such as database username and passwords. A privileged process must be used to get and decrypt encrypted passwords. **Remediation:** Encrypt password used for scheduled jobs and scripts. **Audit:** None	√	√	1 N
12.08	Sensitive information in environment variables on host	Avoid or encrypt	**Rationale:** 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. **Remediation:** Do not store sensitive password in environment variables on the host. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.09	Sensitive information in batch files on host	Avoid or encrypt	**Rationale:** An enforced policy must exist to ensure that no batch files have sensitive information such as database usernames and passwords. A privileged process must be used to get and decrypt encrypted passwords. **Remediation:** Do not store sensitive passwords in batch scripts on the host. **Audit:** None	√	√	1 N
12.10	Oracle file locations	Separate for performance	**Rationale:** If the redo, data, and index files are not properly distributed a single disk failure will cause an Oracle outage and make recovery difficult. **Remediation:** Split the location of the Oracle software distribution, redo logs, data files, and indexes onto separate disks and controllers for resilience. **Audit:** None	√	√	1 S
12.11	File systems	Separate Oracle files from non-Oracle files	**Rationale:** Isolating the Oracle files onto a separate partition enables easier privilege and permissions management. **Remediation:** Only put database files on file systems exclusively used by Oracle. Oracle files must not be on the same partition as the operating system. **Audit:** None	√	√	1 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.12	Optimal Flexible Architecture	Implement	**Rationale:** Systems that are flexible and easy to understand reduce administration complexity and increase overall manageability and security. **Remediation:** Follow the Oracle Optimal Flexible Architecture guidelines to provide for consistency and ease of administration. **Audit:** None	√	√	1 N

12.13	Checksum PL/SQL code	Implement	**Rationale:**
			Maliciously altered stored procedures can compromise Oracle or system security and can go undetected if not properly audited. Store the checksum results upon creation and update of the stored procedure, periodically check for alterations.
			
			Remediation:
			`sha1sum  pl_file.psql`
			
			Audit:
			`sha1sum pl_file.psql`
				√	√	1
						N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.14	All database objects	Monitor	**Rationale:** Maliciously altered objects can compromise Oracle or system security and can go undetected if not properly audited. **Remediation:** 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. **Audit:** None	√	√	1 N
12.15	Ad-hoc queries on production databases	Avoid	**Rationale:** Ad-hoc queries are a direct vector for creating denial of service conditions and possible exploitation of the Oracle database. **Remediation:** Disallow ad-hoc queries on production databases. This recommendation may not be suitable for all environments, for example, data warehouses. Test all queries and provide an application interface for exercising queries on production databases. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.16	Remote shell access on host	Encrypt session	**Rationale:** All remote access from users and administrators to the Oracle host must be encrypted. An attacker on the local network can sniff or intercept unencrypted sessions. **Remediation:** 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. **Audit:** None	√	√	1 N
12.17	Applications with database access	Review	**Rationale:** Allowing unauthorized application access will result in information theft and possible remote compromise of the Oracle database. **Remediation:** Review and control which applications access the database. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.18	Location of development database	Separate server from production database	**Rationale:** Regulatory, compliance, and security best practices require production and test environments to be separate. Test environments generally have lax security and mirror production systems. These can provide a staging point or attack vector for a malicious user if hosted in a single environment. **Remediation:** Test and development databases must not be located on the same server as the production system. **Audit:** None	√	√	1 N
12.19	Network location of production and development databases	Separate	**Rationale:** Regulatory, compliance, and security best practices require production and test environments to be separate. Test environments generally have lax security and mirror production systems. These can provide a staging point or attack vector for a malicious user if hosted in a single network. **Remediation:** If possible, place production databases on a different network segment from test and development databases. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.20	Monitor for development on production databases	Prevent development on production databases	**Rationale:** Development of applications on production databases violates security best practices and leaves debugging and other information useful to an attacker on the production host. **Remediation:** Check for evidence of development occurring on production databases. **Audit:** None	√	√	1 N
12.21	Access to production databases	Avoid access from development or test databases	**Rationale:** Allowing a user to alter a production database from a development or test environment creates a vector for an attacker. Production and test database should remain separate then synced when necessary. **Remediation:** Database access from development and test databases to production databases must be prohibited. **Audit:** None	√	√	1 N
12.22	Developer access to production databases	Disallow	**Rationale:** Developers must not have direct access to production databases. Allowing developers direct access to production databases violates regulator, compliance, and security best practices. **Remediation:** Remove login or authentication means for direct developer access. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

12.23	Developer accounts on production databases	Remove developer accounts	**Rationale:**
			Remove any developer accounts that exist in the production database.
			
			Remediation:
			`userdel <account>`
			
			Audit:
			`cat /etc/passwd`
				√	√	1
						N

12.24	Databases created from production exports	Change passwords	**Rationale:** 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. **Remediation:** Maintain separate user accounts for test and production databases and hosts. **Audit:** None	√	√	1 N
12.25	Databases created from production systems	Remove sensitive data	**Rationale:** 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. **Remediation:** Remove all sensitive data from production hosts before granting access to tester and developers. Clear tables that contain PII, password hashes, or other sensitive data. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.26	Account Management	Document and enforce account management procedures	**Rationale:** 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. **Remediation:** Document the system of controls and checks that surround management procedures. **Audit:** None	√	√	1 N
12.27	Change Control	Document and enforce change control procedures	**Rationale:** 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. Utilization of ticketing system or other Change management system will help facilitate this process. **Remediation:** Adoption of a change management system. **Audit:** None	√	√	1 N
12.28	Disaster recovery procedures	Review	**Rationale:** Disaster recovery procedures must be fully documented and regularly tested. **Remediation:** Review the disaster recovery procedures. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.29	Backdoors	Eliminate	**Rationale:** Tight change control management procedures and checksums of the source code can help prevent backdoors into the database. **Remediation:** Review or audit source code both in development and deployed to production systems. **Audit:** None	√	√	1 N
12.30	Public dissemination of database information	Disallow	**Rationale:** Exposing internal configuration information gives an attacker a list of targets and vectors into the Oracle environment. **Remediation:** The posting of database information such as SIDs, hostnames, and IP addresses to newsgroups and mailing lists must not be allowed. **Audit:** None	√	√	1 N
12.31	Screen saver	Set screen saver/lock with password protection of 15 minutes.	**Rationale:** Desktop screens left unlocked create a vector for attacker to take control of the access granted to the user. **Remediation:** If an organizational policy does not exist, 15 minutes must be set as the standard. **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.32	Distribution of tnsnames.ora files to clients	Include only necessary `tnsnames.ora` when distributing to clients	**Rationale:** If clients connect to the database using tnsnames.ora files, ensure that only necessary entries are included in the file when distributing to clients. Providing additional information about database configuration provides a list of hosts and instances to target and violates security best practices. **Remediation:** Remove entries from `tnsnames.ora` **Audit:** None	√	√	1 N
12.33	Event and System Logs	Monitor	**Rationale:** Excessive or exotic errors may be an indicator of a system or database under attack. Proper log auditing and review is a must to maintain system integrity. **Remediation:** Windows Event Logs and Unix System logs must be regularly monitored for errors related to the Oracle database. **Audit:** None	√	√	1 N
12.34	Access to database objects by a fixed user link	Disallow	**Rationale:** Fixed user database links that have a hard coded username and password must be avoided. Anyone with permissions or rights to view the hard coded username or password exposes that account to unnecessary risk. **Remediation:** Remove username and password **Audit:** None	√	√	1 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.35	Oracle Installation	Oracle software owner account name NOT 'oracle'	**Rationale:** Do not name the Oracle software owner account 'oracle' as it is very well known and used in many automated attacks and brute forcing tools. **Remediation:** Upon oracle installation create a separate user account with the username other than Oracle. **Audit:** None	√	√	2 S
12.36	Oracle Installation	Separate users for different components of Oracle	**Rationale:** Properly privilege separate user accounts associated with each Oracle service. In the event that an Oracle service is compromised privilege separating each service will help reduce the damage an attacker can perform. **Remediation:** 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. **Audit:** None		√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.37	Alerts on high priority incidents	Create processes to alert	**Rationale:** Monitoring high priority incidents will help in the event of a security incident. **Remediation:** Create processes to monitor and alert on high priority incidents. **Audit:** None	√	√	2 N
12.38	Intelligent agent	Do not use	**Rationale:** Intelligent agents provide a direct management interface to the Oracle database. **Remediation:** 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. **Audit:** None	√	√	2 N
12.39	Network	Implement if appropriate	**Rationale:** Traffic sent unencrypted across a network can be monitored and intercepted **Remediation:** If appropriate to the environment, implement Oracle Advanced Security to encrypt all traffic between the client and server, OAS solutions include IPSec and mutually authenticated SSL. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.40	Application PL/SQL code	Encrypt	**Rationale:** The wrap program provided by Oracle encodes the PL/SQL source code but does not encrypt it. **Remediation:** Encrypt the PL/SQL code, do not rely on the wrap functionality to protect highly sensitive information. **Audit:** None	√	√	2 N
12.41	Hard coded data in PL/SQL and application source code	Avoid or encrypt	**Rationale:** Do not use unencrypted hard coded usernames, passwords, or other critical data in the PL/SQL code. PL/SQL code is often viewable by many users of the Oracle system and stored in code repositories. **Remediation:** Avoid hardcoded data in code. Use a secure data storage mechanism. Strip all sensitive information from PL/SQL code before storage into a repository. **Audit:** None	√	√	2 N
12.42	Decommissioned applications	Remove all components	**Rationale:** Failure to remove all privileges once an application has been removed from an Oracle database widens the attack surface and can provide unmonitored access for an attacker. **Remediation:** Ensure that all associated binaries, users, batch process, and access rights are removed when applications are decommissioned. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.43	DDL statements in application	Disallow	**Rationale:** Applications must not alter the database schema. **Remediation:** Only allow updates of the database schema though a DBA or approved change management system. **Audit:** None	√	√	2 N
12.44	Host and Application Monitoring Software.	Review	**Rationale:** Any remote access to the database host must be controlled by an application level firewall. **Remediation:** Block unnecessary ports used for monitoring and remote interfaces to the Database. This includes operations management consolidation suites. **Audit:** None	√	√	2 N
12.45	Enabling of batch process account	Time enabled	**Rationale:** Allowing the batch account to remain active widens the system attack surface and may lead to unauthorized access of the Oracle database. **Remediation:** The account that is used to run batch processes must be enabled only during the time that the batch processes run. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.46	Passwords for batch processes	Secure	**Rationale:** Passwords for batch processes must not be a command line parameter or an environment variable. **Remediation:** Remove passwords from batch files and scripts; ensure that passwords are not set as environment variables. **Audit:** None	√	√	2 N
12.47	External account access for batch processes	Disallow	**Rationale:** External accounts used for batch processes allow a simple way to access the database. **Remediation:** Forbid the usage of batch process to access the Oracle database. **Audit:** None	√	√	2 N
12.48	User permissions	Review	**Rationale:** Review and test development databases for users with excess permissions not granted in production. **Remediation:** Restrict test development databases. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.49	Procedures for backup tape retrieval	Review	**Rationale:** Loss of a tape can compromise other measures taken to protect database information. **Remediation:** Ensure the procedures for backup tape retrieval are documented and are adequate to prevent social engineering attacks to steal data. **Audit:** None	√	√	2 N
12.50	Intrusion detection system on host	Utilize	**Rationale:** A host based intrusion detection system provides another layer of defense for the Oracle server. **Remediation:** Use a host based Intrusion Detection System on the server hosting the Oracle database. **Audit:** None	√	√	2 N
12.51	Remote Administration of Listener	Use encryption if remote administration is required.	**Rationale:** 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. **Remediation:** `SECURE_CONTROL_listener_name=(TCPS,IPC)` **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.52	Multiple listeners	Create separate listeners for clients and administration. Protect the administrative listener with IPSec ESP or OAS SSL and a host-based firewall.	**Rationale:** An administrative listener, protected by IPSec, could allow administrators access to the server if the client listener(s) fail.. Preference of implementation is IPSec ESP, otherwise SSL and host-based firewall. If SSL is not possible, use OAS native encryption/integrity with a host firewall.. Access must be limited to specific administrative workstations. **Remediation:** Create separate listeners for clients and administration. Protect the administrative listener with IPSec ESP, SSL or OAS . and a host firewall. **Audit:** None	√	√	2 N
12.53	Policy Caching	Policy caches must be purged.	**Rationale:** 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. **Remediation:** Purge policy caches. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.54	Policy Functions	Users should not have execute, alter or drop privileges on policy functions.	**Rationale:** The ability to manipulate policy functions could be used to defeat row level security. **Remediation:** Users should not have `EXECUTE`, `ALTER` or `DROP` privileges on policy functions. **Audit:** None	√	√	2 N
12.55	Passwords	Remove password parameters from configuration files utilized for Silent Installations.	**Rationale:** Whenever utilizing silent installs, i.e., Oracle Installer, ensure configuration files do not contain password values after the installation completes. **Remediation:** Remove all passwords post installation. **Audit:** None	√	√	2 N
12.56	DataGuard Auth	Authenticate Data Guard with SSL Certificates	**Rationale:** Strong authentication using certificates provides both security and identification of endpoints for the DataGuard service. **Remediation:** Connections between Data Guard servers should be authenticated using SSL certificates **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
12.57	Data Guard Mode	Select Maximum Protection	**Rationale:** Loss of data can result in the loss of system integrity or audit trails. Setting Data Guard to maximum mode ensures no information is lost in the event of a failure. **Remediation:** If possible configure Data Guard for Maximum Protection to ensure that zero data loss occurs if a primary database fails. **Audit:** None	√	√	2 N
12.58	Data Guard Redo	Authenticate Redo Transport Services using SSL Certificates	**Rationale:** Connections sent across the network unencrypted can be monitored and intercepted exposing sensitive information. **Remediation:** Connections for Redo services should be authenticated using SSL certificates. **Audit:** None	√	√	2 N
12.59	Incident Packages	Ensure Incident Packages are destroyed or properly protected after upload to Oracle.	**Rationale:** Sensitive information may be contained in incident packages. Not sanitizing packages may result in leaking of sensitive information to Oracle. **Remediation:** Ensure the minimal amount of sensitive information is sent to Oracle and destroy Incident Packages after submission. **Audit:** None	√	√	2 N

13. Auditing Policy and Procedures

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
13.01	Auditing	Unused schemas should be dropped	**Rationale:** Leaving additional schemas in the database can provide an attacker with additional details about the currently used Oracle system or contain sensitive information. **Remediation:** Unused schemas should be first audited to ensure that they are in fact unused. After verification, they should be dropped. **Audit:** None	√	√	2 N
13.02	Auditing	Trap autonomous transactions	**Rationale:** This will ensure that audit captures actions performed by users even if they are later rolled back. **Remediation:** None **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.03	Auditing	Audit all logons and logoffs.	**Rationale:**
			Auditing logon and logoff events may provide additional information for isolating the cause of security incidents.
			
			Remediation:
			`AUDIT CREATE SESSION`
			
			Audit:
			`SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE SESSION'`
			
			Note: This is audited by default when default security settings are enabled.
				√	√	2
						S

13.04	Auditing	Audit for unsuccessful attempts. Audit by `ACCESS WHENEVER NOT SUCCESSFUL`.	**Rationale:** 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. **Remediation:** Ex. `AUDIT SELECT ON TABLE WHENEVER NOT SUCCESSFUL` **Audit:** `SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME='<OBJECT_NAME>';`	√	√	2 S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.05	Auditing	Where appropriate or required by security or legal requirements, engage and use the Fine-Grained Auditing (FGA) feature.	**Rationale:**
			The flexibility, column specific sensitivity, SQL capturing, and event handler capabilities of FGA provide auditors and security personnel with valuable information.
			
			Note: The FGA record entry can be pre-qualified. Therefore, it should not add a significant burden to the size of audit records.
			
			Remediation:
			`DBMS_FGA.ADD_POLICY(`
			`<Policy config>`
			`);`
			
			Audit:
			`SELECT policy_name FROM DBA_AUDIT_POLICIES;`
				√	√	2
						S

13.06	Auditing	Where appropriate or required by security or legal requirements, use enhanced capabilities of Fine-Grained Auditing.	**Rationale:**
			FGA has the ability to execute event driven procedures that may allow security and operations teams to receive real time indications of threats. 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.
			
			Remediation:
			`DBMS_FGA.ADD_POLICY(`
			`<Policy config>`
			`);`
			
			Audit:
			`SELECT policy_name FROM DBA_AUDIT_POLICIES`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
13.07	Auditing	Audit `ALTER ANY TABLE`	**Rationale:** Unauthorized table alters can results in application failures or be the precursor to an attack. **Remediation:** Audit `ALTER ANY table;` **Audit:** `SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='ALTER ANY TABLE';`	√	√	2 S

13.08	Auditing	Audit `ALTER USER`	**Rationale:**
			Unauthorized user alters can results in application failures, hijacked credentials, or be the precursor to an attack.
			
			Remediation:
			`AUDIT ALTER USER;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='ALTER USER';`
				√	√	2
						S

13.09	Auditing	Audit any `CREATE` statement	**Rationale:**
			Auditing the creation of objects, such as tables or databases, will provide a record of events that may be useful when investigating security events.
			
			Remediation:
			`AUDIT CREATE ANY <object>;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION LIKE('CREATE%');`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.10	Auditing	Audit `CREATE ROLE`	**Rationale:**
			Auditing the creation of roles will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events.
			
			Remediation:
			`AUDIT CREATE ROLE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='CREATE ROLE';`
				√	√	2
						S

13.11	Auditing	Audit `CREATE USER`	**Rationale:**
			Auditing the creation of users will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events.
			
			Remediation:
			`AUDIT CREATE USER;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='CREATE USER';`
				√	√	2
						S

13.12	Auditing	Audit `CREATE SESSION`	**Rationale:**
			Audit the use of `CREATE SESSION` for successful or unsuccessful operations. This information is also useful for debugging application and user session failures.
			
			Remediation:
			`AUDIT CREATE SESSION;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE UDIT_OPTION='CREATE SESSION;`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.13	Auditing	Audit any `DROP` statement	**Rationale:**
			Auditing the removal of database objects, such as tables or databases, will provide a record of events that may be useful when investigating security events.
			
			Remediation:
			`AUDIT DROP {PRIV};`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION LIKE('DROP%');`
				√	√	2
						S

13.14	Auditing	Audit `DROP ANY PROCEDURE`	**Rationale:**
			Audit the use of `DROP ANY PROCEDURE`. Auditing the removal of database procedures, will provide a record of actions that may be useful when investigating security events.
			
			Remediation:
			`AUDIT DROP ANY PROCEDURE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='DROP PROCEDURE';`
				√	√	2
						S

13.15	Auditing	Audit `DROP ANY TABLE`	**Rationale:**
			Audit the use of `DROP ANY TABLE`. Auditing the removal of database tables, will provide a record of actions that may be useful when investigating security events.
			
			Remediation:
			`AUDIT DROP ANY TABLE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='DROP ANY TABLE';`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.16	Auditing	Audit `GRANT ANY PRIVILEGE`	**Rationale:**
			Auditing the grants will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events.
			
			Remediation:
			`audit GRANT ANY PRIVILEGE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='GRANT ANY PRIVILEGE';`
				√	√	2
						S

13.17	Auditing	Audit `GRANT ANY ROLE`	**Rationale:**
			Auditing the grants will provide a record to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events.
			
			Remediation:
			`AUDIT GRANT ANY ROLE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='GRANT ANY ROLE';`
				√	√	2
						S

13.18	Auditing	Audit `INSERT` failures	**Rationale:**
			Auditing failed inserts may provide be useful when investigating certain security events, such as SQL injections attempts.
			
			Remediation:
			`AUDIT INSERT ON objectname WHENEVER NOT SUCCESSFUL;`
			
			Audit:
			`SELECT OBJECT_NAME, INS, FROM DBA_OBJ_AUDIT_OPTS;`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.19	Auditing	Audit `EXECUTE PROCEDURE`	**Rationale:**
			Audit `EXECUTE PROCEDURE` failures attempted into critical data objects. Auditing the EXECUTE PROCEDURE will provide a record of the procedures that were executed and by whom. This information is also useful when investigating a security event
			
			Remediation:
			`AUDIT EXECUTE PROCEDURE;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='EXECUTE PROCEDURE';`
				√	√	2
						S

13.20	Auditing	Audit `SELECT ANY DICTIONARY`	**Rationale:**
			Audit the use of the `SELECT ANY DICTIONARY`. Auditing `SELECT ANY DICTIONARY` will provide a record of access to DICTIONARY views. This information is also useful when investigating a security event.
			
			Remediation:
			`AUDIT SELECT ANY DICTIONARY;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='SELECT ANY DICTIONARY';`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status

13.21	Auditing	Audit `GRANT ANY OBJECT`	**Rationale:**
			Audit the use of the `GRANT ANY OBJECT`. Auditing the grants will provide a record of the scope of the user object rights to ensure the appropriate use of account administration privileges. This information is also useful when investigating certain security events.
			
			Remediation:
			`AUDIT GRANT ANY OBJECT;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='GRANT ANY OBJECT';`
				√	√	2
						S

13.22	Auditing	Audit `CREATE {ANY} LIBRARY`	**Rationale:**
			Audit the use of the `CREATE LIBRARY PRIVILAGE`
			
			Remediation:
			`AUDIT CREATE LIBRARY;`
			
			Audit:
			`SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='CREATE LIBRARY';`
				√	√	2
						S

13.23	Auditing	Logon, logoff, database start or stop, and other information.	**Rationale:** Specific database application components may contain sensitive information and require more scrutiny or certain events to alarm when triggered. Evaluate applications on a case by case basis and create where appropriate. **Remediation:** Create triggers against all tables and system events that are meaningful to the database and application. **Audit**: None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
13.24	Auditing	Use triggers to implement row level auditing	**Rationale:** If specific rows of data need to be audited create triggers to alarm on auditable events. This will reduce the overall system resources for auditing specific tables and help reduce false alarms. **Remediation:** Use triggers to enforce row level auditing for important data. **Audit:** None	√	√	2 N
13.25	Auditing	Review procedures and reports to review audit logs	**Rationale:** Regular, timely reviews of the collected audit information must be done to ensure system security and integrity. **Remediation:** Assign administrative or DBA time to review report generation logic. **Audit**: None	√	√	2 N

13.26	Auditing	Set `AUDIT ALL ON SYS.AUD$ BY ACCESS`	**Rationale:**
			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.
			
			Remediation:
			`AUDIT ALL ON SYS.AUD$ BY ACCESS;`
			
			Audit:
			`SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME='AUD$';`
				√	√	2
						S

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
13.27	Auditing	Regularly purge the audit trail	**Rationale:** Archive and delete the audit trail as necessary or in line with local data administration policies. The audit trail can consume substantial system resources leading to a denial of services. **Remediation:** Review the purging procedures to ensure that the audit trail is purged regularly. **Audit:** None	√	√	2 N
13.28	Auditing	Audit Exposed Web Services	**Rationale:** Legacy procedures that are designed for internal usage only are often exposed as web services. Both the legacy status and expansion of the attack surface can lead to their exploitation. **Remediation:** Audit any XML DB or PL/SQL procedures that have been exposed as web services. **Audit:** None	√	√	2 N

Appendix A – Additional Settings (not scored)

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.01	Oracle Label Security	Where possible use Oracle Label Security.	**Rationale:** 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. **Remediation:** Where possible enable and apply Oracle label security. This can be cost prohibitive depending on licensing with Oracle. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.02	Oracle Label Security	Hide label column.	**Rationale:** 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 copies, and then removes 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. **Remediation:** 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` procedure (for a specific table). Note: After applying a OLS policy to a table, the hidden status of the labels cannot be revoked without the loss of the labels. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.03	Oracle Label Security	Include `LABEL_UPDATE`	**Rationale:** This ensures the user cannot reclassify the data in the record by changing the label. **Remediation:** Include the `LABEL_UPDATE` as a value for `TABLE_OPTIONS` parameter when the OLS policy is applied to a table. **Audit:** None	√	√	2 N
14.04	Oracle Label Security	Limit manipulation.	**Rationale:** 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. **Remediation:** Where possible, use a trusted procedure to limit and control the manipulation of the labels. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.05	Oracle Label Security	Backup data.	**Rationale:** 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. **Remediation:** Have a secure and separate data copy before implementing OLS. **Audit:** None	√	√	2 N
14.06	Oracle Label Security	Where applicable and possible, store labels in the Oracle Internet Directory (OID).	**Rationale:** In the context of the 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. **Remediation:** Where applicable and possible, store labels in the Oracle Internet Directory (OID). **Audit:** None	√	√	2 N
14.07	RAID file systems	Implement	**Rationale:** File systems holding the Oracle data should be on RAID volumes for resilience. **Remediation:** Create RAID partitions for the Oracle database and files. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.08	Magnetically wipe failed disks	Implement	**Rationale:** Sensitive data or information can be recovered from magnetic or data media if not properly erased. **Remediation:** Magnetically wipe old, no longer used, or failed disks. This issue is most likely handled by system administrators. **Audit:** None	√	√	2 N
14.09	Backups on system disks	Verify permissions	**Rationale:** 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. **Remediation:** Set proper permissions on oracle data files stored on backup tapes. **Audit:** None	√	√	2 N
14.10	Off site backup storage	Implement	**Rationale:** It is a best practice to have redundant offsite backups in the event of a physical catastrophe. **Remediation:** Implement off site backup storage procedures. **Audit:** None	√	√	2 N

Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	Windows	Unix	Level & Score Status
14.11	Recovery procedures	Document and Test	**Rationale:** Failure to properly implement and test recovery procedures can result in loss of data and compromise system integrity. **Remediation:** Ensure that database recovery procedures are fully documented and regularly tested. **Audit:** None	√	√	2 N
14.12	Screening router	Implement to restrict access to database host	**Rationale:** Unrestricted access to the database widens the attack surface. Network access should be limited to application and administrative hosts. **Remediation:** Implement a screening router to restrict access to the database host. **Audit:** None	√	√	2 N
14.13	Host-based firewall	Implement on database administration machines	**Rationale:** Use a host based firewall on all computers used to remotely administer databases. **Remediation:** None **Audit:** None	√	√	2 N

Appendix B – Acknowledgments

The contributions to the consensus process made by the following people were instrumental in the creation of this guide:

- Sheila Christman
- Dana Hemlock
- Chad Hughes
- Brian P. McDonald
- Alf-Ivar Holm
- Don Granaman

Appendix C – 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 D – Using Enterprise Manager Grid Control for Patch and Policy Management

The Oracle 11g 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® Database 2 Day DBA 11g Release 1 (11.1) Part Number B28301-02*

Patching Setup:

The Oracle 11g Enterprise Manager Grid Control application can be set up to automatically access Oracle MetaLink to search for and download any new patches available for your Oracle installs. The administrator can then schedule and apply the patch(es) to any host in the enterprise.

Policy Violations:

The Oracle 11g 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.

Appendix E -- Change History

Version	Date	Changes
1.0	9/12/2008	- Initial Public Release