Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

Security Configuration Benchmark

CIS Oracle Database Server 11g R2 on Windows

v1.0.0

Export Date 09-20-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document is intended to address the recommended security settings for the Oracle 11g, r2 Database ©, running on either an x86 (32-bit) or x64 (64-bit) AMD/Intel chip platform. Specifically, the requirements included in this document have been designed for and tested against the Intel x64 chip running a 32-bit version of Microsoft Windows 2008 Server ©, configured as a stand-alone system, with only the default installation and domain membership, and the installation of all [Windows] service packs up through April 15, 2012. Future Windows 2008 patches/service packs or Oracle 11g r2 critical patch updates (CPUs) may impact the recommendations included in this document.

To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Oracle Database Server 11g R2 on Windows Server 2008.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Alan Covell, *Qualys, Inc*

Editor
Stephen Willis, *Qualys, Inc*

Recommendations

1 System-specific settings for the Windows OS

The Windows Operating system is quite different from the UNIX flavors, which are still targeted to operate primarily on CLI interfaces. There are obvious trade-offs, but Windows is GUI by nature so it can allow a greater ease of use for the database novice to more quickly learn the system. Applications of the Windows OS patch/security packs levels will not be addressed here, but it is important to remember that certain of these patches/updates may conflict with or compromise the security recommendations listed below, as well as impacting any legacy applications that must run simultaneously with current or prior versions of Oracle.

1.1 Do not install Oracle on a Domain Controller (DC) (Scored)

Profile Applicability:

- Level 1

Description:

The Windows DC carries all of the user authentication and profile information of the Windows domain.

Rationale:

Not installing the Oracle instance on the DC will reduce the potential attack surfaces of both systems, as both require certain open ports to operate and could present multiple opportunities for denial-of-service or privilege-escalation attacks.

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.
```

Remediation:

Create a stand-alone server for the Oracle instance.

1.2 Use a Restricted Services Account for the Oracle Installation (Not Scored)

Profile Applicability:

- Level 1

Description:

The Restricted Services Account (RSA) limits actions that can be taken that will affect the local system and lacks any significant administrative rights on a Windows domain, so it will not affect surrounding systems if it is compromised in some way

Rationale:

Installing the Oracle instance with an RSA will reduce both the potential for successful attacks and having an attack spread beyond the one system.

Audit:

Determine the account type of the Oracle account using the following script:

```
C:\> Some script that prints out the Oracle account type
```

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.

1.3 Use a Restricted Services Account for Oracle domain installation (Not Scored)

Profile Applicability:

- Level 1

Description:

The Restricted Services Account (RSA) limits actions that can be taken that will affect the local system and lacks any significant administrative rights on a Windows domain, so it will not affect surrounding systems if it is compromised in some way

Rationale:

Whenever the Oracle instance needs domain services, installing it an RSA will reduce both the potential for successful attacks and having an attack spread beyond the one system and into the domain.

Audit:

Determine the account type of the Oracle account using the following script:

```
C:\> Some script hat prints out the Oracle account type
```

Remediation:

Run the Oracle services using a local administrator account created specifically for Oracle. Use the account created to install the product.

1.4 Assign "Deny Logon locally" to the Oracle account (Scored)

Profile Applicability:

- Level 1

Description:

Rationale:

Audit:

Remediation:

1.5 Create a Global Group for the Oracle RSA account (Scored)

Profile Applicability:

- Level 1

Description:

Creating a specific Windows Global Group that limits group membership for the Oracle RSA account limits interactions with other global groups in the Windows domain where the

Oracle instance is located. This limited global group will not have administrative rights on any other domain servers.

Rationale:

Whenever the Oracle instance needs domain services, installing it in an RSA its own group will help prevent unnecessary interactions with other global/local groups, to reduce both the potential for successful attacks and having an attack launched against the Oracle instance from spreading beyond the one system and into the domain.

Audit:

Determine if any groups contain the Oracle RSA with the following procedure:

```
C:\ Some script that prints out RSA group membership on the Oracle host.
```

Remediation:

Use the account creation tool to ensure that no domain rights are assigned beyond the minimum to install and operate the database instance.

1.6 Remove the Oracle RSA for the "Domain Users" account (Scored)

Profile Applicability:

- Level 1

Description:

The "Domain Users" accounts opens up a list of domain's resources, such as list/read access for file server storage, print capability on print servers, a flattening of network subnet accesses, and so on. Allowing the Oracle RSA account to have standard domain access should be unnecessary for the instance's operations.

Rationale:

Whenever the Oracle instance needs domain services, granting resource access permissions back one at a time is much safer than granting this capability as the "Blanket access" of "Domain Users." As removing the Oracle system will reduce both the potential for successful domain attacks and having an attack launched against the Oracle instance, this value should be set according to the needs of the organization.

Audit:

On a DC, display the properties of the Oracle object, with following procedure:

```
C:\dsget user <OracleUserDN> -memberof
Ensure Domain Users is not listed.
```

Remediation:

Use the Account Manager to remove the Oracle RSA from the "Domain Users" group.

1.7 Limit the Oracle account's Domain Network Permissions (Scored)

Profile Applicability:

- Level 1

Description:

Unless there has been a radical change in Operations that this writer is unaware of, the sort of network limitation implied here has generally been done through router and firewall configuration, not Windows account/group configuration or settings.

Rationale:

Audit:

Remediation:

1.8 Limit the Oracle account's logon to the Oracle system only (Not Scored)

Profile Applicability:

- Level 1

Description:

The Oracle DB system should have very few users that have access to the system through an OS-based account that relies on system "authentication, authorization, and accounting" (AAA) of user activity.

Rationale:

The Oracle instance should rely primarily on its DB-based AAA processes for user access, nearly all of which should be from remote locations. As restricting the domain access of the Oracle RSA to the Oracle system alone can help prevent cross-corruption of domain resources, this value should be set according to the needs of the organization.

Audit:

```
C:\> Some script to check for login capabilities on other systems
```

Remediation:

Use the Windows Account Manager to ensure the login is restricted to the local system.

1.9 Limit access to the Oracle directory (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle DB system directory, containing all configuration files/settings should not require access except for the administrator, system, and oracle-specific OS accounts.

Rationale:

The Oracle instance should have all of its files in a single location for monitoring and access controls. As restricting access to the Oracle files on the system to the absolute minimum of accounts can help prevent file corruption or theft of proprietary information, these permissions should be set according to the needs of the organization.

Audit:

```
C:\> script for permissions on "%ProgramFiles\Oracle"
```

Remediation:

Remove the `BUILTIN\Users` group and any other accounts not required for DB operations from the file permissions.

1.10 Limit access permissions to the Windows Registry Key for Oracle (Scored)

Profile Applicability:

- Level 1

Description:

Oracle's Windows Registry Key specifies the specific environments and settings for DB system operations. No one should require access to these configurations except for the administrator, system, and oracle-specific OS accounts.

Rationale:

The Oracle instance's operations draw all configuration settings from its Windows Registry Key. As restricting access to this key to the absolute minimum of accounts can help prevent instance corruption or alteration of the security profile, these permissions should be set according to the needs of the organization.

Audit:

```
C:\> Some script to show the current RegKey settings
```

Remediation:

```
C:\> Some script to set the current RegKey settings
```

1.11 Set the OSAUTH prefix in Oracle's Windows Registry Key (Scored)

Profile Applicability:

- Level 1

Description:

Oracle's Windows Registry Key specifies the specific environments and settings for DB system operations. No one should require access to these configurations except for the administrator, system, and oracle-specific OS accounts.

Rationale:

The Oracle instance's operations draw all configuration settings from its Windows Registry Key and subkeys. As requiring that the system's domain name be part of the username for externally authenticated accounts strengthens the authentication requirements, this value should be set according to the needs of the organization.

Audit:

```
C:\> Some script to show the current RegKey settings for the
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES\OSAUTH_PREFIX_DOMAIN value
```

Remediation:

```
C:\> Some script to change the current RegKey settings for the
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\ALL_HOMES\OSAUTH_PREFIX_DOMAIN value
```

1.12 Set the OSAUTH prefix in Oracle's Windows Registry Key (Scored)

Profile Applicability:

- Level 1

Description:

Oracle's Windows Registry Key specifies the specific environments and settings for DB system operations. No one should require access to these configurations except for the administrator, system, and oracle-specific OS accounts.

Rationale:

The Oracle instance's OS operations draw all configuration settings from its Windows Registry Key and subkeys. As requiring that client connections flow through a single port allows for more consistent connection monitoring and firewall protection settings, this value should be set according to the needs of the organization.

Audit:

```
C:\> Some script to show the current RegKey settings for the
HKEY_LOCAL_MACHINE\ SOFTWARE\ORACLE\HOME<#>\USE_SHARED_SOCKET value
```

Remediation:

```
C:\> Some script to change the current RegKey settings to
HKEY_LOCAL_MACHINE\ SOFTWARE\ORACLE\HOME<#>\USE_SHARED_SOCKET --> TRUE
```

1.13 Verify permissions for all Oracle-associated files on the system (Not Scored)

Profile Applicability:

- Level 1

Description:

Oracle's application files/programs are critical to the control of the database instance and protecting the proprietary information in the database.

Rationale:

As weak permissions settings on Oracle files can allow the corruption the database instance and cause a Denial-of-Service condition and/or data loss, the permissions on the Oracle files should be set according to the needs of the organization.

Audit:

```
C:\> Some script to show the permissions for Oracle files that do not have the
"oracle," "SYSTEM," and "Administrators" as the sole permissions holders.
```

Remediation:

```
C:\> Change the Oracle file permissions to allow full access to SYSTEM, oracle, and
Administrators and remove the Domain Users and Everybody groups.
```

1.14 Verify permissions for third-party programs on the Oracle system (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

There are cases where legacy/maintenance applications are required for database system operations, having both the database and third-party application files/programs (other than ones directly Oracle- or OS-based) loaded onto the same system as Oracle.

Rationale:

As the Oracle instance's database and/or OS operations can potentially be corrupted by manipulations of third-party software that has weak permissions, these third-party software directory permissions should be set according to the needs of the organization.

Audit:

```
C:\> Some script to show the current directory permissions for third-party programs
(non-Oracle/OS) on the Oracle system under "Program Files"
```

Remediation:

```
C:\> Change the setting for current directory permissions on third-party programs to
exclude unnecessary user permissions.
```

1.15 Separate the partitions for Oracle and third-party software (Not Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Ideally, the Oracle installation would be on its own system. At minimum, no applications and/or programs should share the system partitions with the database instance(s) except for oracle-specific OS files required for system operations.

Rationale:

As the Oracle instance's database and/or OS operations can potentially be corrupted by hidden vulnerabilities in third-party software loaded onto the same disk partitions as Oracle, this structuring should be established according to the needs of the organization.

Audit:

```
C:\> Some script to show the current location of system HDD partitions, with all top-
level directories listed.
```

Remediation:

```
Ensure that non-Oracle and non-OS software is not stored on the Oracle partition.
```

1.16 Verify permissions for the DBMS_OBSFUCATION_TOOLKIT (Scored)

Profile Applicability:

- Level 1

Description:

The `DBMS_OBSFUCATION_TOOLKIT` settings provide one of the tools that determine the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. (The DES (56-bit key) and 3DES (168-bit key) are the two types available and `PUBLIC` is granted the `EXECUTE` permission by default.) The encryption functions of the

DBMS_OBSFUCATION_TOOLKIT have been replaced by the DBMS_CRYPTO package, but the prior one has been kept for backwards compatibility.

Rationale:

As encrypted data storage procedures can become a Denial-of-Service if unauthorized users with PUBLIC privileges encrypt the data stream to an unknown key, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine if PUBLIC has EXECUTE privileges for  the
DBMS_OBSFUCATION_TOOLKIT setting
```

Remediation:

```
C:\>REVOKE EXECUTE ON  DBMS_OBSFUCATION_TOOLKIT to PUBLIC;
```

2 Oracle Database Installation and Patching Requirements

[This space intentionally left blank]

2.1 Ensure installation limits access to $TMP/$TMPDIR to Oracle (Not Scored)

Profile Applicability:

- Level 1

Description:

During the Oracle installation, the database can potentially create temporary files or settings with PUBLIC privileges.

Rationale:

As these temporary files or settings with PUBLIC privileges can potentially be altered and/or subverted by any connected user, limitations on connections other than those required for the installation during setup should be established according to the needs of the organization.

Audit:

```
C:\> Some script to determine if the $TMP and $TMPDIR environment variables are set to
protected directories with access limited to the software owner and the ORA_INSTALL
group.
```

Remediation:

```
Change the $TMP and $TMPDIR environment variables to protected directories that limit
access to the software owner and the ORA_INSTALL group.
```

2.2 Ensure the latest version/patches for Oracle software is installed (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle installation version, along with the patch level, should be the most recent that is compatible with the organizations' operational needs.

Rationale:

As using the most recent Oracle database software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software, the installation version and/or patches applied during setup should be established according to the needs of the organization.

Audit:

```
C:\> opatch lsinventory -detail
```

Remediation:

```
Check the results of opatch against the current list of Oracle patches on metalink
```

2.3 Ensure that only required Oracle components are installed (Not Scored)

Profile Applicability:

- Level 1

Description:

The Oracle installation has a great many components, not all of which are needed for the organization's operational tasks.

Rationale:

As installing more Oracle database capabilities than are absolutely required can expose vulnerabilities in the unnecessary portions of the software, the installation should be limited according to the needs of the organization.

Audit:

```
C:\> Some script showing all installed Oracle program capabilities
```

Remediation:

```
Uninstall those Oracle program capabilities that are not required for operational
tasks
```

2.4 Ensure the Oracle tkprof tool is removed from Production (Scored)

Profile Applicability:

- Level 1

Description:

The TKPROF program allows conversion of the trace files into a human-readable text, to allow diagnostics of database problem areas.

Rationale:

As retaining TKPROK on a Production system could allow an unauthorized user to discover database weaknesses, it should be removed or restricted according to the needs of the organization.

Audit:

```
C:\> Some script to check for the presence of the TKPROF utility.
```

Remediation:

```
Remove TKPROF entirely.
```

2.5 Ensure the Oracle listener default name is changed (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle `listener` provides network connections to the database with the name of the connection, protocol addresses, and services offered by the database.

Rationale:

As the default name of the listener is well known and could facilitate network-based Denial-of-Service attacks against its bandwidth capabilities, it should be renamed according to the needs of the organization.

Audit:

```
C:\> Some script to check for the default value of the listener
```

Remediation:

```
Change the default name of the listener
```

2.6 Ensure the Oracle listener file uses IPs instead of hostnames (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle `listener` provides network connections to the database with the name of the connection, protocol addresses, and services offered by the database. The `listener.ora` file can contain connection information based on host names or IP addresses.

Rationale:

As using host names in `listener.ora` file could allow DNS server cache-poisoning to facilitate a network-based Denial-of-Service attacks on the system, the requisite hostnames should be listed as IP addresses, according to the needs of the organization.

Audit:

```
C:\> Some script to check for hostnames in the listener.ora file
```

Remediation:

```
Change the hostnames in the listener.ora file to IP addresses
```

*2.7 Ensure the Oracle otrace *.dat files are removed (Scored)*

Profile Applicability:

- Level 1

Description:

The Oracle "Trace" (otrace) utility provides a way to trace SQL statement executions, as well as data on the duration, frequency, and resources the database uses for all parse, execution, and fetch events

Rationale:

As the `*.dat` files generated by the `otrace` utility contain sensitive information that could facilitate attacks on the system, these should be removed according to the needs of the organization.

Audit:

```
C:\> Some script to check for the presence of *.dat files on the system
```

Remediation:

```
Remove the *.dat files from the $ORACLE_HOME directory
```

2.8 Ensure there are no passwords in the listener.ora file (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle `listener` provides network connections to the database with the name of the connection, protocol addresses, and services offered by the database. In database versions prior to 11gr2, there was an option to include a password in the `listener.ora` file or to have OS-based authentication for `listener` connections; now only OS-based authentication is allowed and `listener.ora` file password use has been deprecated.

Rationale:

As using the default OS-based authentications for `listener` connections can remove the need to include a clear-text password in the `listener.ora` file, any password in this file should be removed according to the needs of the organization.

Audit:

```
C:\> Some script to check for the presence of legacy passwords in the listener.ora
file
```

Remediation:

```
Remove any legacy passwords from the listener.ora file
```

2.9 Ensure the installation exposes no Oracle default accounts (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle installation creates a number of well-known default accounts, "locking and expiring" these (excepting the SYS, SYSMAN, and SYSTEM accounts) to prevent exploitation of the account privileges by unauthorized users.

Rationale:

As the default accounts created by Oracle can provide a point for access by unauthorized users, the remaining accounts should be "locked and expired" according to the needs of the organization.

Audit:

```
C:\> Some script to check the locked/expired status of the default Oracle accounts
```

Remediation:

```
Remove or lock/expire the default Oracle accounts
```

2.10 Ensure all Oracle default accounts have passwords changed (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle installation creates a number of well-known default accounts, "locking and expiring" these (excepting the SYS, SYSMAN, and SYSTEM accounts) to prevent exploitation of the account privileges by unauthorized users.

Rationale:

As the default accounts created by Oracle have well-known passwords and can provide a point for access by unauthorized users if unlocked, all the default accounts remaining after unnecessary ones have been deleted, should have the default passwords changed according to the needs of the organization.

Audit:

```
C:\> Some script to check the default password status of the default Oracle accounts
```

Remediation:

```
Change the passwords of the Oracle default accounts after completing the installation.
```

2.11 Remove unnecessary Oracle default accounts (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle installation creates a number of well-known default accounts, "locking and expiring" these (excepting the SYS, SYSMAN, and SYSTEM accounts) to prevent exploitation of the account privileges by unauthorized users.

Rationale:

As the default accounts created by Oracle can provide a point for access by unauthorized users, the remaining accounts should be "locked and expired" according to the needs of the organization.

Audit:

```
C:\> Some script to check for the existence of unnecessary default Oracle accounts
```

Remediation:

```
Remove unnecessary default Oracle accounts
```

2.12 Remove unnecessary OEM objects (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle installation provides the Oracle Enterprise Manager (OEM) GUI interface for managing one of more database/instances, but is not necessarily required for managing a given database or its role in operations.

Rationale:

As the Oracle Enterprise Manager (OEM) interface generally functions as a point for access to a number of database instances and can use a significant amount of system resources, this should be used or removed according to the needs of the organization.

Audit:

```
C:\> Some script to check for the existence of OEM
```

Remediation:

```
Remove the OEM if unnecessary
```

2.13 Change the default port numbers that connect to Oracle (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle installation creates a number of well-known ports for connections to the listener service, which are often the targets of automated exploits by unauthroized users.

Rationale:

As the default ports created by Oracle can provide a target for exploits by unauthorized users, the ports should be changed according to the needs of the organization.

Audit:

```
C:\> Some script to check for ports 1521 and 1528 in listener.ora
```

Remediation:

```
Change listener port numbers
```

2.14 Ensure third-party accounts put on Oracle get new passwords (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

Various third-party programs create well-known defaults accounts on the Oracle database during their installation, which leaves them open to exploitation of the account privileges by unauthorized users.

Rationale:

As the default accounts created on Oracle by third-party software often have well-known passwords and can provide a point for access by unauthorized users if the passwords are unchanged, all the accounts remaining after unnecessary ones have been deleted or locked should have the default passwords changed according to the needs of the organization.

Audit:

```
C:\> Some script to check the default password status of the third-party accounts
installed on Oracle.
```

Remediation:

```
Change the passwords of the third-party accounts installed on Oracle.
```

2.15 Change the Oracle default service identifier (sid) (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle installation creates a default site identifier number

Rationale:

As the default ports created by Oracle can provide a target for exploits by unauthorized users, the ports should be changed according to the needs of the organization.

Audit:

```
C:\> select instance from v$thread
```

Remediation:

```
Change the sid
```

2.16 Change the name of the default Oracle account if necessary (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle installation requires a software account owner.

Rationale:

As the use of the name "oracle" for the software account owner is well known and provides a target for exploits by unauthorized users, the name of this account should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine if an account named "oracle" is present on the system
```

Remediation:

```
Change the software owner account name
```

3 Oracle Directory and File Permissions

[This space intentionally left blank]

3.1 Verify/set ownership of the $ORACLE_HOME/bin directory (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `ORACLE_HOME/bin` directory contains all the primary system binaries.

Rationale:

As lax permissions on this directory could allow unauthorized users to alter/substitute the directory contents to launch exploits, access should be restricted according to the needs of the organization.

Audit:

```
C:\> some cacls script to determine if the Administrator and Oracle RSA are the owners
of the ORACLE_HOME/bin directory
```

Remediation:

```
Change the ownership of the directory to the limit it to the  Oracle RSA
```

3.2 Verify/set permissions for the init.ora file (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `init.ora` file contains all the primary system startup (init) settings. This file is stored in the `%ORACLE_HOME%\database` directory and can have between 200-300 instance startup parameters.

Rationale:

As lax permissions on this file could allow unauthorized users to alter/substitute the contents of the file to launch exploits, access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine if the Oracle RSA is the owner of the init.ora file
```

Remediation:

```
Change the ownership of the file to the limit it to the Oracle RSA
```

3.3 Verify/set permissions for the sp.ora file (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

When creating an Oracle database via the Database Configuration Assistant, a "Server Parameter File" (SPFILE) is created from the "Initialization Parameter File," then the initialization parameter file is renamed. Oracle will not recognize the former initialization file on future DB startups, nor is it used after the instance is started. This new SPFILE is located in the `ORACLE_BASE\ORACLE_HOME\database` directory by default. The new SPFILE filename is `spfile`*`SID`*`.ora`.

The `sp.ora` file contains all the Oracle Database configurations for the Automatic Storage Management (ASM) instance in a separate server parameter file (SPFILE). .

Rationale:

As lax permissions on this file could allow unauthorized users to overwrite the file to launch exploits, access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions on the
ORACLE_BASE\ORACLE_HOME\database\spfile.ora file
```

Remediation:

```
Change the ownership of the file to limit the "write" permissions to the Oracle and
dba accounts.
```

3.4 Verify/set permissions for the database datafiles (.dbs) (Scored)*

Profile Applicability:

- Level 1

Description:

The ORACLE_HOME/dbs directory contains configuration files, such as the "`/u01/oracle/prod/rbs01.dbs`", "`/u01/oracle/prod/users01.dbs`", and "`/u01/oracle/prod/temp01.dbs`" which hold sensitive user information.

Rationale:

As lax permissions on this directory could allow unauthorized users to overwrite the files to launch exploits, access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions on the \ORACLE_HOME\dbs directory
```

Remediation:

```
Change the ownership of the file to limit the "write" permissions to the Oracle and
dba accounts.
```

3.5 Verify/set permissions for any files listed as an ifile target (Scored)

Profile Applicability:

- Level 1

Description:

The `IFILE` setting is used to embed another parameter, to specify an alternate file target for a prior location, within the `init.ora` file.

Rationale:

As lax permissions on any target file(s) listed as IFILE=* could allow unauthorized users to overwrite the file(s) listed as IFILES and launch exploits, access to these should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the existence of IFILE targets in init.ora and then list
the permissions
```

Remediation:

```
Change the ownership of the IFILE target file to limit  permissions to the Oracle and
dba accounts.
```

3.6 Verify/set permissions for the audit_file_dest file target (Scored)

Profile Applicability:

- Level 1

Description:

The `audit_file_dest` log file in `init.ora` target specifies the location where the DB instance's audit dump files are stored. It is also the location where the `audit_sys_operations`, records for the full auditing of SYS, are written.

Rationale:

As lax permissions on `audit_file_dest` file target could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt the log files, access to the log file should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the name of the audit_file_dest file target and return
the file permissions
```

Remediation:

```
Change the ownership of the audit_file_dest file target limit permissions to the
Oracle and dba accounts.
```

3.7 Verify/set permissions for the diagnostic_dest file target (Scored)

Profile Applicability:

- Level 1

Description:

The `diagnostic_dest` file parameter identifies the location of the Automatic Diagnostic Repository (ADR), which contains data such as the alert log, dumps, [db health] monitor reports, and traces.

Rationale:

As lax permissions on `audit_file_dest` file target could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt the log files, access to the log file should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the name of the diagnostic_dest file target and return
the file permissions
```

Remediation:

```
Change the ownership of the diagnostic_dest file target and limit permissions to the
Oracle and dba accounts.
```

3.8 Verify/set permissions for the control_files file target (Scored)

Profile Applicability:

- Level 1

Description:

The database `control_files` parameter sets the "physical" structure of the database in the way a complex building's creation is specified by engineering drawings. The `*.ctl` file's contents are absolutely essential to the DB's operation and may contain, but are not limited to the following:

- Archive log mode setting,
- Archive log history,
- DB information (RESETLOGS SCN and their time stamp),
- DB name,
- Redo log threads, and
- Tablespace/datafile records-- checkpoints, filenames, on/offline, etc.

Rationale:

As lax permissions on the `control_files` file targetscould allow unauthorized users to overwrite the file(s) and launch exploits to corrupt/destroy the database, access to the control files should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the name of the control_files targets in init.ora and
return the file permissions
```

Remediation:

```
Change the ownership of the control_files target and limit permissions to the Oracle
RSA and dba accounts.
```

3.9 Verify/set permissions for the log_archive_dest_n file targets (Scored)

Profile Applicability:

- Level 1

Description:

The `log_archive_dest_n` initialization parameter provides from 1-10 destinations that specify where each of the `LOCATION` or the `SERVICE` attributes are given that point to where redo data will be archived.

Rationale:

As lax permissions on the `log_archive_dest_n`file targets could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt/destroy the database, access to the control files should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the name of the log_arcive_dest_n targets in init.ora
and return the file permissions
```

Remediation:

```
Change the ownership of the log_arcive_dest_n file targets and limit permissions to
the Oracle RSA and dba accounts.
```

3.10 Verify/set permissions on the\%ORACLE_HOME%\network\admin directory files (Scored)

Profile Applicability:

- Level 1

Description:

The `%Oracle_Home%\network\admin` directory holds all the files that are restricted to the `dba` group.

Rationale:

As lax permissions on the `%Oracle_Home%\network\admin` directory could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt/destroy the database, directory access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for
%Oracle_Home%\network\admin
```

Remediation:

```
Change the ownership of the %Oracle_Home%\network\admin directory and limit
permissions to the Oracle RSA and dba accounts/ or group.
```

3.11 Verify/set permissions on the sqlnet.ora file (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlnet.ora` file contains the parameters for communication between the user and the server containing the database instance.

Rationale:

As lax permissions on the `sqlnet.ora` file could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt/destroy the database, file access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for sqlnet.ora file
```

Remediation:

```
Change the ownership of the sqlnet.ora file and limit write permissions to the Oracle
RSA and dba accounts, with read permissions only for all others.  *
```

3.12 Verify/set permissions on the log_directory_client= target (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlnet.ora` file contains many database and system parameters, including the `log_directory_client`= (directory target) as the destination directory for the client's log files.

Rationale:

As lax permissions on the `log_directory_client=`(directory target) could allow unauthorized users to overwrite the client log file(s) and corrupt/obscure any forensic evidence within it, access to this file target access should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for the
log_directory_client=(directory target)  file
```

Remediation:

```
Change the ownership of the log_directory_client=(directory target)  file and limit
write permissions to the Oracle RSA and dba accounts.
```

3.13 Verify/set permissions on the log_directory_server= target (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlnet.ora` file contains many database and system parameters, including the `log_directory_server=`(directory target) to specify the database server's trace file destination directory.

Rationale:

As lax permissions on the `log_directory_server=`(directory target) could allow unauthorized users to overwrite the database server's log file(s) and corrupt/obscure any forensic evidence within it, access to this file target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for the
log_directory_server=(directory target)  file
```

Remediation:

```
Change the ownership of the log_directory_server=(directory target)  file and limit
write permissions to the Oracle RSA and dba accounts.
```

3.14 Verify/set permissions on the trace_directory_client= target (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlnet.ora` file contains many database and system parameters, including the `trace_directory_client=`(directory target) as the client's destination directory for the trace log files.

Rationale:

As lax permissions on the `trace_directory_client=`(directory target) could allow unauthorized users to overwrite the client trace file(s) and corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for the
log_directory_client=(directory target)  file
```

Remediation:

```
Change the ownership of the log_directory_client=(directory target)  file and limit
write permissions to the Oracle RSA and dba accounts.
```

3.15 Verify/set permissions on the trace_directory_server= target (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlnet.ora` file contains many database and system parameters, including the `log_directory_server=`(directory target) to specify the database server's trace file destination directory.

Rationale:

As lax permissions on the `log_directory_server=`(directory target) could allow unauthorized users to overwrite the database server's trace file(s) and corrupt/obscure any forensic evidence within it, access to this file target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the directory permissions for the
log_directory_server=(directory target)  file
```

Remediation:

```
Change the ownership of the log_directory_server=(directory target)  and limit write
permissions to the Oracle RSA and dba accounts.
```

3.16 Verify/set permissions on the listener.ora file (Scored)

Profile Applicability:

- Level 1

Description:

The `listener.ora` file contains the name of the listener file, the network protocol/ address combinations offered by the database services.

Rationale:

As lax permissions on the `listener.ora` file could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the listener.ora  file
```

Remediation:

```
Change the ownership/permissions to the listener.ora and limit permissions to the
Oracle RSA and dba accounts.
```

3.17 Verify/set permissions on the log_file_listener file target (Scored)

Profile Applicability:

- Level 1

Description:

The `log_file_listener=`(file target) is the location of the listener file log, the network protocol/ address combinations offered by the database services.

Rationale:

As lax permissions on the `log_file_listener=`(file target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the log_file_listener=( file target)
```

Remediation:

```
Change the ownership/permissions to the log_file_listener=( file target) and limit
permissions to the Oracle RSA and dba accounts.
```

3.18 Verify/set permissions on the trace_directory_listener_name target (Scored)

Profile Applicability:

- Level 1

Description:

The `trace_directory_file_listener_name=`(directory target) is the location of the directory for listener trace file.

Rationale:

As lax permissions on the `trace_directory_file_listener_name=`(directory target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the
trace_directory_file_listener_name=(directory  target)
```

Remediation:

```
Change the ownership/permissions to the
trace_directory_file_listener_name=((directory  target)  and limit permissions to the
Oracle RSA and dba accounts.
```

3.19 Verify/set permissions on the trace_file_listener_name file target (Scored)

Profile Applicability:

- Level 1

Description:

The `trace_file_listener_name=`(file target) is the location/name of the listener trace file.

Rationale:

As lax permissions on the `trace_file_listener_name=`(file target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the trace_file_listener_name=( file
target)
```

Remediation:

```
Change the ownehip/permissions to the trace_file_listener_name=( file target)  and
limit permissions to the Oracle RSA and dba accounts.
```

3.20 Verify/set permissions on the sqlplus binaries directory (Scored)

Profile Applicability:

- Level 1

Description:

The `sqlplus` binaries support the operations of the Oracle command-line utility program SQL and PL/SQL, which can perform any database operation.

Rationale:

As lax permissions on the `sqlplus` binaries directory could allow unauthorized users to launch exploits against the database, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the sqlplus binaries directory
```

Remediation:

```
Change the ownership/permissions the sqlplus binaries directory restrict access to the
Oracle RSA and dba accounts.
```

3.21 Verify/set permissions on the .htaccess files (Scored)

Profile Applicability:

- Level 1

Description:

The `.htaccess` files support the operations of the Oracle web server program, which can use the file(s) contents to make dynamic changes to the Web server on a per-directory basis, without having to impact the overall server configuration or having to bounce the web server instance. .

Rationale:

As lax permissions on the `.htaccess` files could allow unauthorized users to launch exploits against the webserver and alter data presentation through the web pages, access to the file(s) should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the location(s) and permissions set for the .htaccess
file(s)
```

Remediation:

```
Change the ownership/permissions the .htaccess file(s) to restrict access to the
Oracle RSA and dba accounts.
```

3.22 Verify/set permissions on the dads.conf file (Scored)

Profile Applicability:

- Level 1

Description:

The `dads.conf` file contains the configuration parameters for the PL/SQL Database Access Descriptor (DAD); the DAD values specify how an HTTP request is to be fulfilled/generated by the database server.

Rationale:

As lax permissions on the `dads.conf` file could allow unauthorized users to launch exploits against the database, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the dads.conf binaries directory
```

Remediation:

```
Change the ownership/permissions for the dads.conf directory restrict access to the
Oracle RSA and dba accounts.
```

3.23 Verify/set permissions on the xsqlconfig.xml file (Scored)

Profile Applicability:

- Level 1

Description:

The `xsqlconfig.xml` file contains the configuration parameters for the Oracle XSQL pages "publishing framework," which is an extensible platform for publishing XML in multiple formats. This can allow for the presentation of the same data in multiple formats, such as browsers, cell phones, PDA, etc.

Rationale:

As lax permissions on the `xsqlconfig.xml` file could allow unauthorized users to launch exploits against the database, access to this target should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the dads.conf binaries directory
```

Remediation:

```
Change the ownership/permissions for the dads.conf directory restrict access to the
Oracle RSA and dba accounts.
```

3.24 Remove the EVERYONE access capability to the oracle.exe process (Scored)

Profile Applicability:

- Level 1

Description:

Unlike *nix, where each new Oracle process, such as the Database Writer, Log Writer, and so on spawns a new *nix process, in Windows, the `oracle.exe` process contains all the new processes spawned as subprocesses and these threads are accessible by the `EVERYONE` Group.

Rationale:

As access by the EVERYONE Group could allow unauthorized users to launch exploits against the database processes, this access capability should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions set for the oracle.exe process
```

Remediation:

```
Change the permissions for the oracle.exe process to remove access by the  EVERYONE
Group
```

3.25 Verify/set permissions on the postDBCreation.log file (Scored)

Profile Applicability:

- Level 1

Description:

The postDBCreation.log file contains the printout from the database creation. It also contains a printout of the passwords for the DBSNMP and/or SYSMAN users if either of those two have a password that contains exclamation points.

Rationale:

As printouts of the passwords for the DBSNMP and/or SYSMAN users could allow unauthorized users to launch privilege escalation exploits against the database, access to the postDBCreation.log should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the permissions for the postDBCreation.log file
```

Remediation:

```
Change the ownership/permissions for the postDBCreation.log file t restrict access to
the Oracle RSA and dba accounts.
```

4 Oracle Parameter Settings

The operation of the Oracle database instance is governed by numerous parameters that are set in specific configuration files and are instance-specific in scope. As alterations of these parameters can cause problems ranging from denial -of-service to theft of

proprietary information, these configurations should be carefully considered and maintained.

4.1 Prevent trace files from being read by unauthorized users (Scored)

Profile Applicability:

- Level 1

Description:

The `trace_files_public` setting in `init.ora` determines whether or not the `public` user can read the system's trace file.

Rationale:

As permitting the `public` user to read the instance's trace files file could release sensitive information about instance operations, this value should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the "trace_files_public=" value
```

Remediation:

```
Change the "trace_files_public=" value to FALSE
```

4.2 Settings for the global_names parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `global_names` setting in `init.ora` requires that the name of a database link matches that of the remote database it will connect to.

Rationale:

As not requiring database connections to match the domain that is being called remotely could allow unauthorized domain sources to potentially connect via brute-force tactics, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the " global_names =" value
```

Remediation:

```
Change the "global_names =" value to TRUE
```

4.3 Settings for the remote_os_roles parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `remote_os_authen` setting in the `init.ora` file determines whether or not OS 'roles' with the attendant privileges are allowed for remote client connections.

Rationale:

As permitting OS roles for database connections to can allow the spoofing of connections and permit granting the privileges of an OS role to unauthorized users to make connections, this value should be restricted according to the needs of the organization.

Audit:

```
C:\> some script to determine the " remote_os_authen =" value
```

Remediation:

```
Change the " remote_os_authen " value to FALSE
```

4.4 Settings for the remote_listener parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `remote_listener` setting in the `init.ora` file determines whether or not a valid listener can be established on a system separate from the database instance.

Rationale:

As permitting a remote listener for connections to the database instance can allow for the potential spoofing of connections and that could compromise data confidentiality and integrity, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the " remote_listener =" value
```

Remediation:

```
Change the " remote_listener " value to FALSE
```

4.5 Settings for the audit_trail parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `audit_trail` setting in the `init.ora` file determines whether or not Oracle's basic audit features are enabled. These can be set to "Operating System"(OS), "DB," or "DB EXTENDED."

Rationale:

As enabling the basic auditing features for the Oracle instance permits the collection of data to troubleshoot problems, as well as providing value forensic logs in the case of a system breach, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "audit_trail=" value
```

Remediation:

```
Change the "audit_trail" value to OS
```

4.6 Settings for the os_authent_prefix parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `os_authent_prefix` setting in the `init.ora` file specifies the prefix Oracle uses to authenticate connection attempts. (Oracle concatenates this parameter out of the value of the user's OS account name/password.)

Rationale:

As allowing the use of an authentication prefix can permit the roles of the DBA and OS System Administrators to overlap, violating the principle of separation of duties, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the " os_authent_prefix =" value
```

Remediation:

```
Change the " os_authent_prefix " value to ""  (null)
```

4.7 Settings for the os_roles parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `os_roles` setting in the `init.ora` file permits externally created groups to be applied to database management.

Rationale:

As allowing the OS use external groups for database management could cause privilege overlaps and generally weaken security, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "os_roles=" value
```

Remediation:

```
Change the " os_roles" value to FALSE
```

4.8 Settings for the utl_file_dir parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `utl_file_dir` setting in the `init.ora` file permits the creation of directories that can be read and written to by all users.

Rationale:

As using the `utl_file_dir` to create directories allows the potential manipulation of these directories by unauthorized users, use of this command should be avoided.

Audit:

```
C:\> some script to determine the if the " utl_file_dir  " value is present in
init.ora
```

Remediation:

```
Avoid using the "utl_file_dir  " parameter to create directories use CREATE DIRECTORY
```

4.9 Settings for the redo log physical disk locations (Scored)

Profile Applicability:

- Level 1

Description:

The `LOG_ARCHIVE_DUPLEX_DEST` setting in the `init.ora` file shows the physical location(s) of the redo log files used for system recovery.

Rationale:

As having a separate physical location for the redundant redo logs can help ensure the ability to recover the system transactions in the event of a disk failure, this value should be set to the needs of the organization.

Audit:

```
C:\> some script to determine the if the "LOG_ARCHIVE_DUPLEX_DEST" value is present in
init.ora and the value is NOT the same disk as the ORAHOME
```

Remediation:

```
Specify a disk location for the target of the "LOG_ARCHIVE_DUPLEX_DEST" parameter that
is NOT the same as the ORAHOME location
```

4.10 Settings for successful redo log disk writes (Scored)

Profile Applicability:

- Level 1

Description:

The `LOG_ARCHIVE_MIN_SUCCEED_DEST` setting in the `init.ora` file shows the requirement for the successful writing of redo log information to one r more of the physical location(s) of the redo log files.

Rationale:

As conforming that successful writes to the redundant redo logs do occur as specified, to ensure redo logs are available in the event of a disk failure, this value should be set to the needs of the organization.

Audit:

```
C:\> some script to determine the if the "LOG_ARCHIVE_MIN_SUCCEED_DEST" value is
present in init.ora
```

Remediation:

```
Specify a number GE 1 for successful redo log disk writes
for  "LOG_ARCHIVE_MIN_SUCCEED_DEST" parameter
```

4.11 Settings for the sql92_security parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `sql92_security parameter` setting in the `init.ora` file require a user to have the `SELECT` privilege for a table before being allowed to do `UPDATE` or `DELETE` operations that use a `WHERE` clause on the table; this allow a user to delete table data while blocking possibility of the user being able to guess what other values are in that table.

Rationale:

As blocking users with permissions to one set of data within a table from intuiting the contents of other data can help increase data confidentiality, this value should be set to the needs of the organization (See Caution).

Audit:

```
C:\> some script to determine the if the "sql92_security=TRUE" parameter value is
present in init.ora
```

Remediation:

```
Specify the "sql92_security=TRUE" parameter" is set in init.ora
```

4.12 Settings for the admin_restrictions_listener_name parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `admin_restrictions_listener_name` setting in the `listener.ora` file requires that any attempted alteration of the parameters in the `listener` file be refused unless the listener is then restarted by a privileged user.

Rationale:

As blocking unprivileged users from making alterations of the `listener.ora` file, where remote data/services are specified, will help protect data confidentiality, this value should be set to the needs of the organization.

Audit:

```
C:\> some script to determine the if the "admin_restrictions_listener_name=on"
parameter value is present in listener.ora
```

Remediation:

```
Specify the "admin_restrictions_listener_name=on" is set in listener.ora
```

4.13 Setting for the logging_listener parameter (Scored)

Profile Applicability:

- Level 1

Description:

The `logging_listener` setting in the `listener.ora` file requires that all listener action be logged to create an audit trail.

Rationale:

As the logging of all actions by the listener will create an audit trail that is invaluable to forensic investigations of unauthorized activities, this value should be set to the needs of the organization.

Audit:

```
C:\> some script to determine the if the "logging_listener=" parameter value is
present in listener.ora
```

Remediation:

```
Specify the "logging_listener=on" value is set in listener.ora
```

4.14 Setting for the 07_dictionary_accessibility parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `07_dictionary_accessibility` setting in the `init.ora` file is a database initializations parameter that allows/disallows with the EXECUTE ANY PROCEDURE and SELECT ANY DICTIONARY access to objects in the SYS schema; this functionality was created for the ease of migration from Oracle 7 databases to later versions.

Rationale:

As leaving the SYS schema so open to connection could permit unauthorized access to critical data structures, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the if the "07_dictionary_accessibility=" parameter
value is present in init.ora
```

Remediation:

```
Specify the "07_dictionary_accessibility=FALSE" value is set in init.ora
```

4.15 Setting for the spfile<sid>.ora parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The spfile setting for `dispatchers` in the `spfile<sid>.ora` file provides ports for TCP connections for `ftp` (2100) and locally generated `http` (8080).

Rationale:

As leaving these ports open can provide attack vectors into the database instance, this value should be set/removed according to the needs of the organization.

Audit:

```
C:\> some script to determine the if the spfile<sid>.ora contains any "dispatchers=
(PROTOCOL=TCP)" values
```

Remediation:

```
Remove any "dispatchers= (PROTOCOL=TCP)*" values in the spfile<sid>.ora file
```

4.16 Setting for the AUDIT_SYS_OPERATIONS parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `AUDIT_SYS_OPERATIONS` setting for `dispatchers` in the `init.ora` or `spfile<sid>.ora` file provides for the auditing of all user activities conducted under the `SYSOPER` and `SYSDBA` accounts, which are among the highest privilege levels.

Rationale:

As the separation of duties principle requires that audit records of specific user activities not be accessible by the user in question, no matter how privileged the user, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the if the spfile<sid>.ora or init.ora files contains a
"AUDIT_SYS_OPERATIONS" value
```

Remediation:

```
Set the "AUDIT_SYS_OPERATIONS=TRUE" value in the spfile<sid>.ora or init.ora file
```

4.17 Setting for the inbound_connect_timeout parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `inbound_connect_timeout` setting for in the `listener.ora` file determines how long "half-open" connections will be maintained before the connection is closed by the database.

Rationale:

As the maintenance of half-open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "inbound_connect_timeout" value
```

Remediation:

```
Set the "inbound_connect_timeout=2" value in the listener.ora file
```

4.18 Setting for the tcp.validnode_checking parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `tcp.validnode_checking` setting in the `sqlnet.ora` file allow for the testing of incoming connections to see if these match the "invited" and "excluded" systems list.

Rationale:

As limiting connections to system by listing invited and excluded hosts will sharply limit the number of systems that can connect to the instance, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "tcp.validnode_checking" value in the sqlnet.ora
file
```

Remediation:

```
Set the "tcp.validnode_checking=YES" value in the sqlnet.ora file
```

4.19 Settings for the tcp.invited_nodes parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `tcp.invited_nodes` setting in the `sqlnet.ora` file provides a list, based on hostname and/or ip addresses, of nodes permitted to make incoming connections to the Oracle listener.

Rationale:

As limiting connections to the system by listing invited nodes will sharply limit the number of systems that can connect to the instance, thus reducing attack surfaces, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "tcp.invited_nodes" value in the sqlnet.ora file
```

Remediation:

```
Set the "tcp.invited_nodes =[a-zA-Z0-9_\.*]" value in the sqlnet.ora file
```

4.20 Settings for the tcp.excluded_nodes parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `tcp.excluded_nodes` setting in the `sqlnet.ora` file provides a list, based on hostname and/or ip addresses, of nodes not allowed to make incoming connections to the Oracle listener.

Rationale:

As limiting connections to the system by listing excluded nodes will sharply limit the number of systems that can connect to the instance, thus reducing attack surfaces, this value should be set according to the needs of the organization.

Audit:

```
C:\> some script to determine the "tcp.excluded_nodes" value in the sqlnet.ora file
```

Remediation:

```
Set the "tcp.excluded_nodes =[a-zA-Z0-9_\.*]" value in the sqlnet.ora file
```

4.21 Setting for the sqlnet.inbound_connect_timeout parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `sqlnet.inbound_connect_timeout` setting in the `sqlnet.ora` file determines how long "half-open" connections will be maintained, awaiting the completion of authentication, before the connection is closed by the database.

Rationale:

As the maintenance of half-open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the "sqlnet.inbound_connect_timeout "  value
```

Remediation:

```
Set the "sqlnet.inbound_connect_timeout  =3" value in the listener.ora file
```

4.22 Setting for the sqlnet.expire_time parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `sqlnet.expire_time` setting in the `sqlnet.ora` file determines how long database connections that are inactive remain open, before the connection is expired by the database.

Rationale:

As the maintenance of open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the "sqlnet.expire_time "  value
```

Remediation:

```
Set the "sqlnet.expire_time =10" value in the listener.ora file
```

4.23 Setting account access for the application schema owner (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `application schema owner` represents the Oracle user that owns all database objects in a given application's schema, such as fields, packages, relationships, tables, views, and so on, as well the structural definitions that relate the objects in the database.

Rationale:

As allowing continuous schema owner access can potentially allow an unauthorized user to connect as the schema owner, resulting in the compromise of the entire application, this capability should be disabled/restricted according to the needs of the organization.

Audit:

```
C:\>SELECT <APPLICATION_SCHEMA_OWNER (username)>, ACCOUNT_STATUS FROM DBA_USERS;
```

Remediation:

```
ALTER USER <APPLICATION_SCHEMA_OWNER (username)> ACCOUNT LOCK PASSWWORD EXPIRE;
```

4.24 Setting for the remote_login_passwordfile parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `remote_login_passwordfile` setting in the `init.ora` file specifies whether or not Oracle checks for a password file during login and how many databases can use the password file.

Rationale:

As the use of this sort of password login file could permit unsecured, privileged connections to the database, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the "remote_login_passwordfile "  value
```

Remediation:

```
Set the "remote_login_passwordfile =none" value in the init.ora file
```

4.25 Setting for the SQLNET.ALLOWED_LOGON_VERSION parameter (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The setting for the `SQLNET.ALLOWED_LOGON_VERSION` setting in the `sqlnet.ora` file specifies the versions of the Oracle client that are allowed login privileges.

Rationale:

As the pre-11versions of the Oracle client do not use strong authentication for client login and could allow unauthorized users to break credentials sniffed from the network, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the "SQLNET.ALLOWED_LOGON_VERSION="  value
```

Remediation:

```
Set the "SQLNET.ALLOWED_LOGON_VERSION =11" value in the sqlnet.ora file
```

4.26 PATH settings for the environment variables (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `PATH` settings for Oracle specify the locations that the database will use to access the Oracle software packages.

Rationale:

As an overly broad `PATH` statement could allow rogue processes to access Operating System binaries, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the PATH  value
```

Remediation:

```
Set the "PATH" value in Windows properties screen
```

4.27 CLASSPATH settings for the environment variables (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `CLASSPATH` settings for Oracle specify the locations that the database will use to access the Oracle database `Java` software packages.

Rationale:

As an overly broad `CLASSPATH` statement could allow rogue `Java` processes to access Operating System binaries, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the CLASSPATH  value
```

Remediation:

```
Set the "CLASSPATH" value in listener.ora
```

4.28 Remote Administration via the Oracle Connection Manager (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `REMOTE_ADMIN` settings for the database specifies whether or not a remote Oracle Connection Manager Control utility session would be allowed to access the Oracle Connection Manager

Rationale:

As the allowing Oracle Connection Manager Control utility session to connect remotely could facilitate remote system break-in attempts, this value should be set according to the needs of the organization.

Audit:

```
C:\>script to determine the REMOTE_ADMIN  value in cman.ora
```

Remediation:

```
Set the value in cman.ora to REMOTE_ADMIN=NO
```

4.29 Database release level information query settings in init.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The information about patch/update release number in `init.ora` provides information about the exact patch/update release that is currently running on the database.

Rationale:

As allowing the database to return information about the patch/update release number in `init.ora` could facilitate unauthorized users' attempts to gain access based upon known patch weaknesses, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the init.ora
SEC_RETURN_SERVER_RELEASE_BANNER setting
```

Remediation:

```
Set the SEC_RETURN_SERVER_RELEASE_BANNER=false value in init.ora
```

4.30 Setting the DB_SECUREFILE parameter in init.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The DB_SECUREFILE setting in init.ora determines whether or not Large Object (LOB) files can be de-duplicated, encrypted, or compressed during file creation/update operations.

Rationale:

As setting the DB_SECUREFILE parameter to ALWAYS allows the database to return information about the patch/update release number in init.ora to de-duplicate, encrypt, or compress files at need, while files with a BASIC setting do not have this capability, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the DB_SECUREFILE  setting in
init.ora
```

Remediation:

```
Set the DB_SECUREFILE =ALWAYS value in init.ora
```

4.31 Case-sensitive login requirements setting in init.ora (Scored)

Profile Applicability:

- Level 1

Description:

The SEC_CASE_SENSITIVE_LOGIN_SETTINGS SETTINGS information determines whether or not case-sensitivity is required for passwords during login.

Rationale:

As requiring the database to use case-sensitivity during login increases the symbol space necessary for unauthorized users to successfully complete brute-force login attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the init.ora
SEC_CASE_SENSITIVE_LOGIN_SETTINGS setting
```

Remediation:

```
Set the SEC_CASE_SENSITIVE_LOGIN_SETTINGS=TRUE value in init.ora
```

4.32 Maximum failed logins allowed setting in init.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SEC_MAX_FAILED_LOGIN_ATTEMPTS` parameter determines how many failed login attempts are allowed before Oracle closes the login connection.

Rationale:

As allowing an unlimited number of login attempts for a user connection can facilitate both brute-force login attacks and the occurrence of Denial-of-Service, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the init.ora
SEC_MAX_FAILED_LOGIN_ATTEMPTS setting
```

Remediation:

```
Set the SEC_MAX_FAILED_LOGIN_ATTEMPTS=3 value in init.ora
```

4.33 Bad-packet error handling settings in init.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SEC_PROTOCOL_ERROR_FURTHER_ACTION` setting determines the Oracle's server's response to bad/malformed packets received from the client.

Rationale:

As bad packets received from the client can potentially indicate packet-based attacks on the system, such as "TCP SYN Flood" or "Smurf" attacks, which could result in a Denial-of-Service condition, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the init.ora
SEC_PROTOCOL_ERROR_FURTHER_ACTION setting
```

Remediation:

```
Set the SEC_PROTOCOL_ERROR_FURTHER_ACTION=DROP <2 seconds> or
SEC_PROTOCOL_ERROR_FURTHER_ACTION=DELAY <2 seconds> value in init.ora
```

4.34 Bad-packet error logging settings in init.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SEC_PROTOCOL_ERROR_TRACE_ACTION` setting determines the Oracle's server's logging response level to bad/malformed packets received from the client, by generating `ALERT`, `LOG`, or `TRACE` levels of detail in the log files.

Rationale:

As bad packets received from the client can potentially indicate packet-based attacks on the system, such as "TCP SYN Flood" or "Smurf" attacks, which could result in a Denial-of-Service condition, this diagnostic/logging value for `ALERT`, `LOG`, or `TRACE` conditions should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the init.ora
SEC_PROTOCOL_ERROR_TRACE_ACTION setting
```

Remediation:

```
Set the SEC_PROTOCOL_ERROR_TRACE_ACTION=LOG or SEC_PROTOCOL_ERROR_TRACE_ACTION=ALERT
value in init.ora
```

4.35 Listener configuration control settings in listener.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SECURE_CONTROL_listener_name` setting determines the type of control connection the Oracle server requires for remote configuration of the listener.

Rationale:

As listener configuration changes via unencrypted remote connections can result in unauthorized users sniffing the control configuration information from the network, these control values should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the listener.ora
SECURE_CONTROL_listener_name setting
```

Remediation:

```
Set the SECURE_CONTROL_listener_name=TCPS or SECURE_CONTROL_listener_name=IPC in
listener.ora
```

4.36 Listener administration protocol settings in listener.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SECURE_PROTOCOL_listener_name` setting determines the type of protocol the Oracle server requires for remote administrative connections to the listener.

Rationale:

As administrative connections to the listener via unencrypted remote connections can result in unauthorized users sniffing the administrative information from the network, these protocol values should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the listener.ora
SECURE_PROTOCOL_listener_name setting
```

Remediation:

```
Set the SECURE_PROTOCOL_listener_name=TCPS or SECURE_PROTOCOL_listener_name=IPC in
listener.ora
```

4.37 Listener registration connection settings in listener.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SECURE_REGISTER_listener_name` setting determines the type of protocol the Oracle server requires for remote registration connections to the listener.

Rationale:

As registration connections to the listener via unencrypted remote connections can result in unauthorized users sniffing the registration information from the network, these protocol values should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the listener.ora
SECURE_REGISTER_listener_name setting
```

Remediation:

```
Set the SECURE_REGISTER_listener_name=TCPS or SECURE_REGISTER_listener_name=IPC in
listener.ora
```

4.38 Dynamic listener registration settings in listener.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `DYNAMIC_REGISTRATION_listener_name` setting determines whether or not the Oracle server will accept all registration connections to the listener.

Rationale:

As unauthorized registration connection requests to the listener, which have the same name as a pre-existing instance, if successful, are treated as "valid" RAC or Cluster servers for that instance and load-balance the traffic between the unauthorized and authorized servers, facilitating attacks where unauthorized users can sniff the database transmissions from the network, this capability should be restricted/disabled according to the needs of the organization.

Audit:

```
C:\> script to determine the status of the value for the listener.ora
DYNAMIC_REGISTRATION_listener_name setting
```

Remediation:

```
Set the DYNAMIC_REGISTRATION_listener_name=OFF
```

4.39 External procedure call settings in listener.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `EXTPROCS_DLLS` setting determines whether or not the Oracle server will allow external DLLs and/or libraries to be loaded into the database when external procedures are called. These external procedures work through external routines and allow communication with external applications through PL/SQL.

Rationale:

As allowing external DLLs and/or libraries to be loaded into the database when external procedures are called could allow system security protocols to be overwritten or corrupted, this capability should be restricted/disabled according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the listener.ora EXTPROCS_DLLS setting
```

Remediation:

```
Set the EXTPROCS_DLLS =ONLY
```

5 Encryption-specific Requirements and Settings

The encryption of the contents of the data tables and traffic can help to ensure hat even if the data is compromised by network sniffing or unauthorized access, the data will remain unintelligible to the recipient due to its encrypted state.

5.1 Encryption of server-to-client communications in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.ENCRYPTION_SERVER` setting in `sqlnet.ora` enables the encryption for the database server, which will then allow, reject, request, or require encryption for all client connections.

Rationale:

As the lack of encryption on connection requests could make the traffic vulnerable network sniffers, this capability should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.ENCRYPTION_SERVER setting
```

Remediation:

```
Set the value SQLNET.ENCRYPTION_SERVER =REQUIRED in sqlnet.ora
```

5.2 Encryption of client-to-server communications in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.ENCRYPTION_CLIENT` setting in `sqlnet.ora` enables the encryption for the client to the database server, which will then allow, reject, request, or require encryption for all connections.

Rationale:

As the lack of encryption on connection requests could make the traffic vulnerable network sniffers, this capability should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.ENCRYPTION_CLIENT setting
```

Remediation:

```
Set the value SQLNET.ENCRYPTION_CLIENT =REQUIRED in sqlnet.ora
```

5.3 FIPS-compliant communications setting in fips.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SSLFIPS_140` setting in `sqlnet.ora` enables/disables the requirement for applying the FIPS 140-2 standard to the database server's communications; FIPS must be enabled on both server and client for this to be effective.

Rationale:

As the application of increasing levels of FIPS 140-2 can provide increasing levels of security, including authentication, encryption, and operational conditions, this capability should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the fips.ora SSLFIPS_140 setting
```

Remediation:

```
Set the value SSLFIPS_140 =REQUIRED in fips.ora
```

5.4 Integrity of server-to-client communications in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.CRYPTO_CHECKSUM_SERVER` setting in `sqlnet.ora` specifies the checksum requirement for the database server, which will then accept, reject, request, or require checksumming for all client connections to validate that the datastream is unaltered.

Rationale:

As the lack of checksum integrity checks on traffic can make the datastream vulnerable to undetected alteration, this capability should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.CRYPTO_CHECKSUM_SERVER
setting
```

Remediation:

```
Set the value SQLNET.CRYPTO_CHECKSUM_SERVER in sqlnet.ora
```

5.5 Integrity of client-to-server communications in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.CRYPTO_CHECKSUM_CLIENT` setting in `sqlnet.ora` specifies the checksum requirement for the database client, which will then accept, reject, request, or require checksumming for all server connections to validate that the datastream is unaltered.

Rationale:

As the lack of checksum integrity checks on traffic can make the datastream vulnerable to undetected alteration, this capability should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.CRYPTO_CHECKSUM_CLIENT
setting
```

Remediation:

```
Set the value SQLNET.CRYPTO_CHECKSUM_CLIENT in sqlnet.ora
```

5.6 Type of server-to-client integrity checks in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER` setting in `sqlnet.ora` specifies the checksum requirement type, MD5 or SHA-1, to be used for the database server integrity process.

Rationale:

As the type of checksum used, the older MD5 vs. the stronger SHA-1, can make the datastream integrity validation process stronger or weaker, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER setting
```

Remediation:

```
Set the value SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER in sqlnet.ora
```

5.7 Type of client-to-server integrity checks in sqlnet.ora (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT` setting in `sqlnet.ora` specifies the checksum requirement type, MD5 or SHA-1, to be used for the client's connections to the database server for integrity checking process.

Rationale:

As the type of checksum used, the older MD5 vs. the stronger SHA-1, can make the datastream integrity validation process stronger or weaker, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT setting
```

Remediation:

```
Set the value SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT in sqlnet.ora
```

5.8 Encryption algorithm/strength of server-to-client connections (Scored)

Profile Applicability:

- Level 1

Description:

The `SQLNET.ENCRYPTION_TYPES_SERVER` setting in `sqlnet.ora` enables specific encryption algorithms for the database server, which can include varying strengths of AES, DES, 3DES, and RC4.

Rationale:

As the lack of encryption on connection requests could make data traffic vulnerable network sniffers, the encryption capability should be set at a high enough value to ensure privacy, according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.ENCRYPTION_TYPES_SERVER
setting
```

Remediation:

```
Set the value SQLNET.ENCRYPTION_TYPES_SERVER = (AES|3DES|RC4) >=128 in sqlnet.ora
```

5.9 Encryption algorithm/strength of client-to-server connections (Scored)

Profile Applicability:

- Level 1

Description:

The `SQLNET.ENCRYPTION_TYPES_CLIENT` setting in `sqlnet.ora` enables specific encryption algorithms for the client to connect to the database server, which can include varying strengths of AES, DES, 3DES, and RC4.

Rationale:

As the lack of encryption on connection requests could make data traffic vulnerable network sniffers, the encryption capability should be set at a high enough value to ensure privacy, according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SQLNET.ENCRYPTION_TYPES_CLIENT
setting
```

Remediation:

```
Set the value SQLNET.ENCRYPTION_TYPES_CLIENT =(AES|3DES|RC4) >=128 in sqlnet.ora
```

5.10 Certificate-request key size in the Oracle wallet (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle `wallet` is an encrypted container for storing authentication and/or signing credentials, which can include passwords, the Transparent Data Entry (TDE) master key, PKI private keys, certificates, and trusted certificates needed by SSL.

Rationale:

As a lack of encryption strength for the various keys associated with connection requests and data table encryption could make data more vulnerable to unauthorized access, this value should be set at a high enough value to serve the needs of the organization.

Audit:

```
C:\> script to determine the value of the wallet key size
```

Remediation:

```
Set the value of the wallet key size to x >=2048
```

5.11 Auto-login to the Oracle wallet for SSL connections (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle `wallet`, an encrypted container for storing authentication and/or signing credentials, can be enabled for automatic PKI-based access to services, allowing single sign-on (SSO) access to multiple Oracle databases, without requiring multiple password entries.

Rationale:

As the wallet storage is a secure, centralized location for encryption certificates and can facilitate single sign-on processes by using the "auto-login" feature, which restricts configuration access to the wallet to the user who created it, this value should be set at a according to the needs of the organization.

Audit:

```
C:\> script to determine the wallet's "autologin" value
```

Remediation:

```
Set the value of the wallet "autologin" to enabled.
```

5.12 Secure Sockets Layer (SSL) version setting in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_VERSION` setting in `sqlnet.ora` requires the use of a specific release level/version of SSL to make valid connections using this type of encryption.

Rationale:

As versions of SSL earlier than 3.0 were known to have potential weaknesses in their algorithms, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_VERSION setting
```

Remediation:

```
Set the value SSL_VERSION =3 in sqlnet.ora
```

5.13 Secure Sockets Layer (SSL) cipher suites in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_CIPHER_SUITES` setting in `sqlnet.ora` requires the use of specific encryption algorithms for SSL to make valid connections.

Rationale:

As versions of SSL cipher suites are known to have potential weaknesses in their algorithms, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_CIPHER_SUITES  setting
```

Remediation:

```
Set the value SSL_CIPHER_SUITES = (SSL_DH_anon_WITH_3DES_EDE_CBC_SHA,
SSL_RSA_WITH_AES_256_CBC_SHA
 SSL_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBE_SHA) in sqlnet.ora
```

5.14 certificate Distinguished Name (DN) in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_SEVER_CERT_DN` setting in `sqlnet.ora` provides the full Distinguished Name (DN) used in formal certificate identification, which is provided by a Certificate Authority (CA). The DN contains all of the individual names of the parent entries, going back to the root entry of the directory tree. This information helps block site masquerading.

Rationale:

As the Distinguished Name provided by the Certificate Authority can help prevent site masquerading and traffic interception due to host impersonation, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_SEVER_CERT_DN setting
```

Remediation:

```
Set the DN value in sqlnet.ora
```

5.15 SSL Client certificate usage requirements in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_CLIENT_AUTHENTICATION` setting in `sqlnet.ora` determines whether or not the client is required to authenticate connection requests using SSL.

Rationale:

As strong identification procedures may have limited impact on security unless connection procedures are equally robust, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_CLIENT_AUTHENTICATION setting
```

Remediation:

```
Set the SSL_CLIENT_AUTHENTICATION=TRUE value in sqlnet.ora
```

5.16 Encryption strength for the DBMS_OBSFUCATION_TOOLKIT (Scored)

Profile Applicability:

- Level 1

Description:

The `DBMS_OBSFUCATION_TOOLKIT` settings provide one of the tools that determine the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key) and 3DES (168-bit key) are the only two types available.

Rationale:

As strong identification procedures may have limited impact on security unless encrypted data storage procedures are equally robust, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the DBMS_OBSFUCATION_TOOLKIT setting
```

Remediation:

```
Set the DBMS_OBSFUCATION_TOOLKIT=3DES
```

5.17 Encryption strength for the DBMS_CRYPTO package (Scored)

Profile Applicability:

- Level 1

Description:

The `DBMS_CRYPTO` settings provide a toolset that determines the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key), 3DES (168-bit key), 3DES-2KEY (112-bit key), AES (128/192/256-bit keys), and RC4 are available.

Rationale:

As strong identification procedures may have limited impact on security unless encrypted data storage procedures are equally robust, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the DBMS_CRYPTO setting
```

Remediation:

```
Set the DBMS_CRYPTO setting >=128-bit key
```

5.18 Permissions for the radius.key file (Scored)

Profile Applicability:

- Level 1

Description:

The `radius.key` file in the `ORACLE_BASE\ORACLE_HOME\network\security\` directory contains the shared-secret password (16 characters or less) that is used to participate in the RADIUS client-server authentication, to authenticate remote client connections; this process treats each Oracle server as a Client connecting to the RADIUS server.

Rationale:

As protecting the contents of this file is critical to maintaining the confidentiality of the remote connection process, the file permissions value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the permissions value of the radius.key in the
ORACLE_BASE\ORACLE_HOME\network\security\ directory
```

Remediation:

```
Set the file permissions to allow only read access by administrators/authorized users.
```

5.19 SSL certificate revocation check requirements in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_CERT_REVOCATION` setting in `sqlnet.ora` determines whether or not certificate revocation checks are required to confirm client certificate authenticity prior to client connections.

Rationale:

As the absence of a confirmation on the current status of a Client certificate can mean that the client is no longer authorized to connect to or receive data, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_CERT_REVOCATION setting
```

Remediation:

```
Set the SSL_CERT_REVOCATION=REQUIRED value in sqlnet.ora
```

5.20 SSL certificate Distinguished Name check in sqlnet.ora (Scored)

Profile Applicability:

- Level 1

Description:

The `SSL_SERVER_DN_MATCH` setting in `sqlnet.ora` determines whether or not the Distinguished Name (DN) in the certificate matches the database server's DN.

Rationale:

As the absence of a confirmation of match between the DN for the certificate and the host it resides on can mean tampering with the SSL certificates or the host, with key values in the non-matching certificate being possibly fraudulent or otherwise exposed, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the sqlnet.ora SSL_SERVER_DN_MATCH setting
```

Remediation:

```
Set the SSL_SERVER_DN_MATCH=YES value in sqlnet.ora
```

6 Backup and Disaster Recovery Settings

The use backup and disaster recovery mechanisms can help to ensure that in the event of logical or physical errors on a given database host's media, critical data can be restored to a prior state or integrity on the same or another host, through the use of system redundancies.

This will have to be completely rewritten, as the extant Oracle benchmark has no scorable items listed.

7 Oracle client/user connection and login restrictions

The restrictions on Client/User connections to the Oracle database help block unauthorized access to data and services by setting access restrictions; these security measures help to ensure that successful logins cannot be easily made through brute-force password attacks or intuited by clever social engineering exploits. By the use of a created profile, e.g. "LIMIT," then assigning this profile to a client, the database administrator can set a standard policy for password security to all users assigned the 'LIMIT' profile; however,

this policy can still be overridden by local policy. All values assigned below are the recommended minimums or maximums; higher, more restrictive values can be applied at the discretion of the organization by creating a separate profile to assign to a different user group.

7.1 Restrictions on failed login attempts via a DB profile (Scored)

Profile Applicability:

- Level 1

Description:

The `failed_login_attempts` setting determines how many failed login attempts are permitted before the system locks the user's account.

Rationale:

As repeated failed login attempts can indicate the initiation of a brute-force login attack, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'failed_login_attempts' in the profile name
LIMIT
```

Remediation:

```
Set the 'failed_login_attempts=5' value in sqlnet.ora or
set the 'failed_login_attempts<=5' value in the LIMIT profile and assign it to the
applicable users.
```

7.2 Requirements for account locking (failed logins) via a DB profile (Scored)

Profile Applicability:

- Level 1

Description:

The `PASSWORD_LOCK_TIME` setting determines how many days must pass for the user's account to be unlocked after the set number of failed login attempts has occurred.

Rationale:

As locking the user account after repeated failed login attempts can block further brute-force login attacks, but can create administrative headaches if the account unlocking process always requires DBA intervention, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'PASSWORD_LOCK_TIME' value in the profile
name LIMIT
```

Remediation:

```
Set the 'PASSWORD_LOCK_TIME>=1' value in the LIMIT profile and assign it to the
applicable users.
```

7.3 Restrictions on password use (duration) via a DB profile (Scored)

Profile Applicability:

- Level 1

Description:

The `password_life_time=90` setting determines how long a password may be used before the user is required to be change it.

Rationale:

As allowing passwords to remain unchanged for long periods makes the success of brute-force login attacks more likely, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'password_life_time' value in the profile
named LIMIT
```

Remediation:

```
Set the 'password_life_time<=90' value in the LIMIT profile and assign it to the
applicable users.
```

7.4 Restrictions on password use (history) via a DB profile (Scored)

Profile Applicability:

- Level 1

Description:

The `password_reuse_max` setting determines how many different passwords must be used before the user is allowed to reuse a prior password.

Rationale:

As allowing reuse of a password within a short period of time after the password's initial use can make the success of password-based attacks more likely, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'password_reuse_max' value in the profile
named LIMIT
```

Remediation:

```
Set the 'password_reuse_max>=12' value in the LIMIT profile and assign it to the
applicable users.
```

7.5 Restrictions on password use (reuse) via a DB profile (Scored)

Profile Applicability:

- Level 1

Description:

The `password_reuse_time` setting determines the amount of time in days that must pass before the same password may be reused.

Rationale:

As reusing the same password after only a short period of time has passed makes the success of brute-force login attacks more likely, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the password_reuse_time in the profile named
LIMIT
```

Remediation:

```
Set the password_reuse_time>=730 value in the LIMIT profile and assign it to the
applicable users.
```

7.6 Requirements for account locking (grace time) via a DB profile (Not Scored)

Profile Applicability:

- Level 1

Description:

The `password_grace_time` setting determines how many days must pass after the user's password expires before the user's login capability is locked out.

Rationale:

As locking the user account after the expiration of the password change requirement's grace period can help prevent password-based attack against forgotten or disused accounts, while still allowing the account and its information to be accessible by DBA intervention, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'password_grace_time' value in the profile
name LIMIT
```

Remediation:

```
Set the 'password_grace_time<=5' value in the LIMIT profile and assign it to the
applicable users.
```

7.7 Requirements for limiting EXTERNAL user login capability (Scored)

Profile Applicability:

- Level 1

Description:

The `password='EXTERNAL'` setting determines whether or not a user can be authenticated by a remote OS to access the database.

Rationale:

As allowing remote OS authentication of a user to the database can potentially allow supposed "privileged users" to connect as "authenticated," even when the remote system is compromised, these logins should be disabled/restricted according to the needs of the organization.

Audit:

```
C:\> script to determine if the 'password=EXTERNAL' value is assigned to any DBA_USER
```

Remediation:

```
Change the 'password=EXTERNAL' value for any users to a new value
```

7.8 Requirement for setting the password verification function (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `password_verify_function` determines password settings when a user password is changed at the SQL command prompt.

Rationale:

As requiring users to apply the 11gr2 security features in password creation, such as forcing mixed-case complexity, the blocking of simple combinations, and change/history settings can potentially thwart logins by unauthorized users, this function should be applied/enabled according to the needs of the organization.

Audit:

```
C:\> script to determine if the 'password_verify_function' value is applied to user
password changes
```

Remediation:

```
Change the 'utlpwdmg.sql' script to require users to apply the 'CIS_utlpwdmg.sql'
requirements to password creation
```

7.9 Requirements for limiting user CPU resource allocations (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The CPU_PER_SESSION setting determines how much access time the user's request is granted for access to the CPU's resources; it is measured in hundredth of seconds.

Rationale:

As limiting the amount of time a request can access the CPU will help prevent poorly formed requests or intentional Denial-of-Service attacks from monopolizing CPU resources, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'CPU_PER_SESSION' value in the profile name
LIMIT
```

Remediation:

```
Set the 'CPU_PER_SESSION=' value to an integer lower than 36000 (1 minute) in the
LIMIT profile and assign it to the applicable users.
```

7.10 Requirements for limiting System Global Area resources (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The PRIVATE_SGA (Private System Global Area) setting determines how large the maximum number integer bytes can grow to become in the private space of the SGA.

Rationale:

As limiting the size of the PRIVATE_SGA can help prevent memory resource exhaustion by poorly formed requests or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'PRIVATE_SGA' value in the profile name
LIMIT
```

Remediation:

```
Set the 'PRIVATE_SGA>=15K=<512K' value in the LIMIT profile and assign it to the
applicable users.
```

7.11 Requirements for limiting amount of disk-access per session (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `LOGICAL_READS_PER_SESSION` (Read limitations for disk access) setting determines the maximum number of database blocks that are allowed to be read per session.

Rationale:

As limiting the number of the `LOGICAL_READS_PER_SESSION` can help prevent memory resource exhaustion by poorly formed requests or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'LOGICAL_READS_PER_SESSION' value in the
profile name LIMIT
```

Remediation:

```
Set the 'LOGICAL_READS_PER_SESSION=<50000' value in the LIMIT profile and assign it to
the applicable users.
```

7.12 Requirements for limiting the number of sessions per user (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `SESSIONS_PER_USER` (Number of sessions allowed) determines the maximum number of user sessions that are allowed to be open concurrently.

Rationale:

As limiting the number of the `SESSIONS_PER_USER` can help prevent memory resource exhaustion by poorly formed requests or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'SESSIONS_PER_USER' value in the profile
name LIMIT
```

Remediation:

```
Set the 'SESSIONS_PER_USER =<10' value in the LIMIT profile and assign it to the
applicable users.
```

7.13 Requirements for limiting the connect time for users (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The `CONNECT_TIME` (Duration of user sessions) determines the maximum number of minutes that a user session, active or idle, can be maintained before it is closed.

Rationale:

As limiting the `CONNECT_TIME` can help prevent database resource exhaustion by abandoned sessions or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'CONNECT_TIME' value in the profile name
LIMIT
```

Remediation:

```
Set the 'CONNECT_TIME =<60' value in the LIMIT profile and assign it to the applicable
users.
```

7.14 Requirements for limiting the idle time for users (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The IDLE_TIME (Duration of user sessions) determines the maximum number of minutes that a user session can be maintained without new input before it is closed.

Rationale:

As limiting the IDLE_TIME can help prevent database resource exhaustion by setting limits on apparently abandoned sessions or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

Audit:

```
C:\> script to determine the value of the 'IDLE_TIME' value in the profile name LIMIT
```

Remediation:

```
Set the 'IDLE_TIME =<60' value in the LIMIT profile and assign it to the applicable
users.
```

8 Oracle user access and authorization restrictions

The capability to use database resources at a given level, or user authorization rules, allows for user manipulation of the various parts of the Oracle database; these authorizations must be structured to block unauthorized use and/or corruption of vital data and services, by setting restrictions on user capabilities; these security measures help to ensure that successful logins cannot be easily redirected towards improper and/or unapproved manipulation of the database's constituent parts.

8.1 Limiting user authorizations for the SYSTEM tablespace (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The SYSTEM tablespace contains all the basic system objects for the database, such as the data dictionary tables.

Rationale:

As allowing any user other than SYS to use the SYSTEM tablespace can potentially allow disk resource exhaustion (Denial-of-Service) condition or data dictionary corruption, requiring a tablespace reconstruction from backups, authorization to use the SYSTEM tablespace should limited according to the needs of the organization.

Audit:

```
SELECT USERNAME, DEFAULT_TABLESPACE FROM DBA_USERS;
```

Remediation:

```
ALTER USERDEFAULT_TABLESPACE table;
```

8.2 Limiting application user resources on a production tablespace (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Production Tablespace(s) for users contains all the system space set aside for application users or developers to read/write data to the production database instance.

Rationale:

As allowing any application user or developer user unlimited write capability on an assigned tablespace can potentially allow a disk resource exhaustion (Denial-of-Service) condition, quotas for disk space should set according to the needs of the organization.

Audit:

```
SELECT <USERNAME> FROM DBA_TS_QUOTAS WHERE USERNAME='USER' AND
TABLESPACE_NAME='TABLESPACE_NAME'
```

Remediation:

```
ALTER USER <USERNAME> QUOTA <VALUE> ON <TABLESPACE_NAME>;
```

8.3 Limiting application/user resources on a production tablespace (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Production Tablespace(s) for users contains all the system space set aside for application users or developers to read/write data to the production database instance.

Rationale:

As allowing any application user or developer user unlimited write capability on an assigned tablespace can potentially allow a disk resource exhaustion (Denial-of-Service) condition, quotas for disk space should set according to the needs of the organization.

Audit:

```
SELECT <USERNAME> FROM DBA_TS_QUOTAS WHERE USERNAME='USER' AND
TABLESPACE_NAME='TABLESPACE_NAME'
```

Remediation:

```
ALTER USER <USERNAME> QUOTA <VALUE> ON <TABLESPACE_NAME>;
```

8.4 Limiting authorizations for edition-based upgrade versioning (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle 11gr2 database can have multiple versions of required PL/SQL objects, views, synonyms and triggers within a single schema. This allows database upgrades without significant database down time.

Rationale:

As allowing a non-privileged user the capability to launch the `EDITION` sequence can potentially invalidate all of the PL/SQL code, with the exception of triggers, this capability should be restricted according to the needs of the organization.

Audit:

```
Script to determine the authorizations for the use of the 'EDITION' privilege
```

Remediation:

```
script to set the authorizations for the use of the 'EDITION' privilege to DBA only
```

8.5 Limiting authorizations for the SYS.AUD$ table (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle database `SYS_AUD$` table contains all the audit records for the database of the non-Data Manipulation Language (DML) events, such as `ALTER`, `DROP`, `CREATE`, and so forth. (DML changes need trigger-based audit events to record data alterations.)

Rationale:

As permitting non-privileged users the authorization to manipulate the `SYS_AUD$` table can allow distortion of the audit records, hiding unauthorized activities, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='AUD$';
```

Remediation:

```
C:\> REVOKE ALL ON SYS.AUD$ FROM <USER>;
```

8.6 Limiting authorizations for the SYS.USER_HISTORY$ table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SYS.USER_HISTORY$` table contains all the audit records for the user's password change history. (This table gets updated by password changes if the user has an assigned profile that has password reuse limit set, e.g., `PASSWORD_REUSE_TIME` set to other than `UNLIMITED`.)

Rationale:

As permitting non-privileged users the authorization to manipulate the `SYS.USER_HISTORY$` table can allow distortion of the audit records, potentially hiding unauthorized password changes, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='SYS.USER_HISTORY$';
```

Remediation:

```
REVOKE ALL ON SYS.USER_HISTORY$ FROM <USER>;
```

8.7 Limiting authorizations for the SYS.LINK$ table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SYS.LINK$` table contains all the user's password information and data table link information.

Rationale:

As permitting non-privileged users the authorization to manipulate the `SYS.LINK$` table can allow capture of password information and/or corrupt the primary database linkages, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='LINK$';
```

Remediation:

```
REVOKE ALL ON SYS.LINK$ FROM <USER>;
```

8.8 Limiting authorizations for the SYS.USER$ table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SYS.USER$` table contains the users' hashed password information.

Rationale:

As permitting non-privileged users the authorization to open the SYS.USER$ table can allow the capture of password hashes for the later application of password cracking algorithms to breach confidentiality, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER$';
```

Remediation:

```
REVOKE ALL ON SYS.USER$ FROM <USER>;
```

8.9 Limiting authorizations for the SYS.SOURCE$ table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database SYS.SOURCE$ table contains the linkages between the OBJ$ (Object ID), LINE (Line Number), and SOURCE (Source code line).

Rationale:

As permitting users the authorization to manipulate the SYS.USER$ table can render the references to source code in the data dictionary useless and destroy database integrity, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='SOURCE$';
```

Remediation:

```
REVOKE ALL ON SYS.SOURCE$ FROM <USER>;
```

8.10 Limiting authorizations for the PERFSTAT.STATS$SQLTEXT table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `PERFSTAT.STATS$SQL_SUMMAY` table contains the full text of all executed SQL statements.

Rationale:

As permitting users the authorization to read the `PERFSTAT.STATS$SQL_SUMMARY` table can expose sensitive information such as schema/tablespace names, user IDs, and valid queries/views, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='PERFSTAT.STATS$SQLTEXT';
```

Remediation:

```
REVOKE ALL ON PERFSTAT.STATS$SQLTEXT;
```

8.11 Limiting authorizations to PERFSTAT.STATS$SQL_SUMMARY table (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `PERFSTAT.STATS$SQL_SUMMARY` table contains the full text of the STATSPACK-generated database activities, which, according to level and threshold setting, can include performance data, rollback data, and many other activity indicators.

Rationale:

As permitting users the authorization to read the `PERFSTAT.STATS$SQL_SUMMARY` table can expose sensitive information such as rollback information, schema/tablespace names, user IDs, and associated queries/views, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='PERFSTAT.STATS$SQL_SUMMARY';
```

Remediation:

```
REVOKE ALL ON PERFSTAT.STATS$SQL_SUMMARY;
```

8.12 Limiting user authorizations for the $X tables (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `$X` tables are the SQL interface for viewing the database's memory allocations associated with database operations, such as the "cursor," as this process is operationalized in the SGA and the type and number of the tables can vary in number according to the database installation type.

Rationale:

As permitting users the authorization to manipulate the `$X` tables can expose sensitive database operations to interference or destruction, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, PRIVILEGE TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE ('X$%');
```

Remediation:

```
REVOKE ALL ON X$<TABLENAME> FROM <USER>;
```

8.13 Limiting user authorizations for the DBA_% views (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA_` views are the SQL interface for viewing the database's memory allocations associated with database operations, such as the "cursor," as this process is operationalized in the SGA and the type and number of the tables can vary in number according to the database installation type.

Rationale:

As permitting users the authorization to manipulate the DBA_ views can expose sensitive database operations to interference or destruction, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DICT WHERE TABLE_NAME LIKE ('DBA_%') and user not in ('SYS', 'SYSTEM')
ORDER BY TABLE_NAME;
```

Remediation:

```
REVOKE ALL ON DBA_<TABLENAME> FROM <Non-DBA/SYS USER>;
```

8.14 Limiting user authorizations for the $V_ views (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database $V_ views provide a continually updated look at internal database statistics, with 467 possible views in Oracle 11gr2, including all SQL statements running: The V$ views are sometimes referred to as "Dynamic performance views or tables" for this reason.

Rationale:

As permitting users the authorization to read the $V_ views can expose sensitive database operations that hold information that can facilitate system attacks, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE 'V$_%'
ORDER BY TABLE_NAME;
```

Remediation:

```
REVOKE ALL ON TABLENAME LIKE 'V$_' FROM <Non-SYS USER>;
```

8.15 Limiting user authorizations for the ALL_SOURCE view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `ALL_SOURCE` view describes the "Text source" of the stored objects available to the current user.

Rationale:

As permitting unauthorized viewing of a user's available text source can expose sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='ALL_SOURCE';
```

Remediation:

```
REVOKE ALL ON ALL_SOURCE FROM <Non-DBA USER>;
```

8.16 Limiting user authorizations for the DBA_ROLES view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA_ROLES` view lists all the roles that exist in the database.

Rationale:

As permitting unauthorized access to the `DBA_ROLES` can allow the alteration of sensitive data or bring down the data instance, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBA_ROLES';
```

Remediation:

```
REVOKE ALL ON DBA_ROLES FROM <Non-dba/SYS USER>;
```

8.17 Limiting user authorizations for the DBA_SYS_PRIV view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA_SYS_PRIV` view lists the system privileges granted to users and roles that exist in the database.

Rationale:

As permitting unauthorized access to the `DBA_SYS_PRIV` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DBA_SYS_PRIV';
```

Remediation:

```
REVOKE ALL ON DBA_SYS_PRIV FROM <Non-SYS USER>;
```

8.18 Limiting user authorizations for the DBA_ROLE_PRIV view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA_ROLE_PRIV` view lists the privileges for all the roles that exist in the database.

Rationale:

As permitting unauthorized access to the `DBA_ROLE_PRIV` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DBA_ROLE_PRIV';
```

Remediation:

```
REVOKE ALL ON DBA_ROLE_PRIV FROM <Non-SYS/DBA USER>;
```

8.19 Limiting user authorizations for the DBA_TAB_PRIV view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA_TAB_PRIV` view lists the user privileges for all the tables that exist in the database.

Rationale:

As permitting unauthorized access to the `DBA_TAB_PRIV` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DBA_ROLE_PRIV';
```

Remediation:

```
REVOKE ALL ON DBA_ROLE_PRIV FROM <Non-SYS/DBA USER>;
```

8.20 Limiting user authorizations for the ROLE_ROLE_PRIVS view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `ROLE_ROLE_PRIVS` view lists all the roles granted to other roles and is limited to the roles which the current user can access.

Rationale:

As permitting unauthorized access to the `ROLE_ROLE_PRIVS` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='ROLE_ROLE_PRIVS';
```

Remediation:

```
REVOKE ALL ON ROLE_ROLE_PRIVS FROM <Non-SYS/DBA USER>;
```

8.21 Limiting user authorizations for the USER_TAB_PRIVS view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `USER_TAB_PRIVS` view lists all the granted table privileges for all users in the database.

Rationale:

As permitting unauthorized access to the `USER_TAB_PRIVS` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='USER_TAB_PRIVS';
```

Remediation:

```
REVOKE ALL ON USER_TAB_PRIVS FROM <Non-SYS/DBA USER>;
```

8.22 Limiting user authorizations for the USER_ROLE_PRIVS view (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `USER_ROLE_PRIVS` view lists all the granted role privileges for all users in the database.

Rationale:

As permitting unauthorized access to the `USER_ROLE_PRIVS` view can allow the disclosure of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='USER_ROLE_PRIVS';
```

Remediation:

```
REVOKE ALL PRIVILEGES ON USER_ROLE_PRIVS FROM <Non-SYS USER>;
```

8.23 Limiting user authorizations for the SELECT_CATALOG role (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SELECT_CATALOG` role provides `SELECT` privileges on all data dictionary views held in the `SYS` schema..

Rationale:

As permitting unauthorized access to the `SELECT_CATALOG` role can allow the disclosure of all dictionary data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='SELECT_CATALOG';
```

Remediation:

```
REVOKE ALL ON SELECT_CATALOG FROM <Non-SYS USER>;
```

8.24 Limiting user authorizations for the SELECT_CATALOG_ROLE (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SELECT_CATALOG_ROLE` provides `SELECT` privileges on all data dictionary views held in the `SYS` schema.

Rationale:

As permitting unauthorized access to the `SELECT_CATALOG_ROLE` can allow the disclosure of all dictionary data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='SELECT_CATALOG_ROLE';
```

Remediation:

```
REVOKE ALL ON SELECT_CATALOG_ROLE FROM <Non-SYS USER>;
```

8.25 Limiting user authorizations for the EXECUTE_CATALOG role (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `EXECUTE_CATALOG_ROLE` provides `EXECUTES` privileges for packages and procedures in the data dictionary in the `SYS` schema.

Rationale:

As permitting unauthorized access to the `EXECUTE_CATALOG_ROLE` can allow the disruption of operations by initialization of rogue procedures, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='EXECUTE_CATALOG_ROLE';
```

Remediation:

```
REVOKE ALL ON EXECUTE_CATALOG_ROLE FROM <Non-SYS USER>;
```

8.26 Limiting user authorizations for the DELETE_CATALOG_ROLE (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DELETE_CATALOG_ROLE` provides `DELETE` privileges for the records in the system's audit table (`AUD$`).

Rationale:

As permitting unauthorized access to the `DELETE_CATALOG_ROLE` can allow the destruction of audit records vital to the forensic investigation of unauthorized activities, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DELETE_CATALOG_ROLE';
```

Remediation:

```
REVOKE ALL ON DELETE_CATALOG_ROLE FROM <Non-SYS USER>;
```

8.27 Limiting user authorizations for the RECOVERY_CATALOG_ OWNER (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `RECOVERY_CATALOG_OWNER` provides full privileges to the `RECOVERY CATALOG`, which is a database schema that tracks backups and stores the commands used for RMAN-based backup and recovery situations.

Rationale:

As permitting unauthorized access to the RECOVERY_CATALOG_OWNER can allow the covert or overt destruction of system backup data and procedures, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='RECOVER_CATALOG_OWNER';
```

Remediation:

```
REVOKE ALL ON RECOVER_CATALOG_OWNER FROM <Non-SYS/USER>;
```

8.28 Limiting user authorizations for the $V synonym(s) (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database $V synonyms are the pointers used to access the $V_ views and provide a continually updated look at internal database statistics, with 467 possible views in Oracle 11gr2, including all SQL statements currently running: The $V_ views are sometimes referred to as "Dynamic performance views or tables" for this reason.

Rationale:

As permitting users the authorization to read the $V synonyms can expose sensitive database operations that hold information that can facilitate attacks, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE 'V$_%'
ORDER BY TABLE_NAME;
```

Remediation:

```
REVOKE ALL ON TABLENAME LIKE 'V$_' FROM <Non-SYS USER>;
```

8.29 Limiting basic user privileges to CREATE_SESSION (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `CREATE_SESSION` privilege provides basic connection capabilities for the standard "Application user" to establish a session with the database so that further specific privileges for DDL, written into the application routines, can take over; when running the "`select * from dba_sys_privs`" statement on a default installation of Oracle 11gr2 Enterprise, it can return more than 700 rows of privilege assignments.

Rationale:

As access to the myriad privileges beyond `CREATE_SESSION` can allow an unauthorized user to potentially view confidential data or do harm to the database instance(s), all privileges beyond this capability, should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE_SESSION' and USER not in ('SYS',
'SYSTEM') order by 1;
```

Remediation:

```
REVOKE ALL PRIVS DBA_SYS_PRIVS WHERE PIVILEGE NOT=('create session') AND USER <Non-sys
USER>  (NEEDS WORK)
```

8.30 Limiting basic user privileges to restrict the ANY keyword (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `ANY` keyword provides the user the capability to alter any item in the catalog of the database, such as `USER` or `SESSION`.

Rationale:

As authorization to use the `ANY` can allow an unauthorized user to potentially change confidential data or damage the data catalog, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE ('%ANY%') and USER NOT IN ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE ALL ON '%ANY%' FROM USER NOT IN ('SYS', 'SYSTEM');
```

8.31 Limiting users by restricting GRANT_ALL_PRIVILEGES (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `GRANT_ALL_PRIVILEGES` keyword provides the user the capability to grant privileges to any item in the catalog of the database.

Rationale:

As authorization to use the `GRANT_ALL_PRIVILEGES` privileges keyword can allow an unauthorized user to potentially access/change confidential data or damage the data catalog, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT_ALL_PRIVILEGE' and USER not in
('SYS', 'SYSTEM') order by 1;
SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT_ANY_OBJECT_PRIVILEGE' and USER not
in ('SYS', 'SYSTEM') order by 1;
```

Remediation:

```
REVOKE ALL ON DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT_ANY_OBJECT_PRIVILEGE' and USER not
in ('SYS', 'SYSTEM');
```

8.32 Limiting users by restricting the EXEMPT_ACCESS_POLICY (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `EXEMPT_ACCESS_POLICY` keyword provides the user the capability to access all the table rows regardless of row-level security lockouts.

Rationale:

As assignment of the `EXEMPT_ACCESS_POLICY` privilege can allow an unauthorized user to potentially access/change confidential data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXEMPT_ACCESS_POLICY' and USER not in
('SYS', 'SYSTEM');
```

Remediation:

8.33 Limiting users by restricting the WITH_ADMIN privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `WITH_ADMIN` privilege allows the designated user to grant another user the same privileges.

Rationale:

As assignment of the `WITH_ADMIN` privilege can allow the granting of a restricted privilege to an unauthorized user, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS WHERE ADMIN_OPTION='YES' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE <ROLE> from <USER>;
GRANT <ROLE> to <USER>;
```

8.34 Limiting users by restricting the WITH_GRANT privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `WITH_GRANT` privilege allows the designated user to grant another user the same privilege(s) he/she holds.

Rationale:

As assignment of the `WITH_GRANT` privilege can allow the granting of a restricted privilege to an unauthorized user, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTABLE='YES' and USER not in ('SYS', 'SYSTEM');
```

Remediation:

```
REVOKE <ROLE> from <USER>;
GRANT <ROLE> to <USER>;
```

8.35 Limiting users by restricting the CREATE privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `CREATE` privilege allows the designated user to create tables, objects, and views.

Rationale:

As assignment of the `CREATE` privilege can allow the creation of numerous database objects and potentially lead to a Denial-of-Service condition, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS FROM PRIVILEGE LIKE ('%CREATE%') and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE CREATE <PRIV> <ROLE> from <USER/ROLE>;
```

8.36 Limiting users by restricting the CREATE LIBRARY privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `CREATE LIBRARY` privilege allows the designated user to create objects that are associated to shared libraries.

Rationale:

As assignment of the `CREATE LIBRARY` privilege can allow the creation of numerous library-associated objects and potentially corrupt the libraries' integrity, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='CREATE LIBRARY' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE CREATE LIBRARY from <USER/ROLE>;
```

8.37 Limiting users by restricting the ALTER SYSTEM privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `ALTER SYSTEM` privilege allows the designated user to dynamically alter the instance's running operations.

Rationale:

As assignment of the `ALTER SYSTEM` privilege can lead to severe problems, such as the instance's session being killed or the stopping of redo log recording, which would make transactions unrecoverable, this capability should be severely restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='ALTER SYSTEM' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE ALTER SYSTEM from <USER/ROLE>;
```

8.38 Limiting users by restricting the CREATE PROCEDURE privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `CREATE PROCEDURE` privilege allows the designated user to create a stored procedure that will fire when given the correct command sequence.

Rationale:

As assignment of the `CREATE PROCEDURE` privilege can lead to severe problems in unauthorized hands, such as rogue procedures facilitating data theft or Denial-of-Service by corrupting data tables, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='CREATE_PROCEDURE' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE CREATE_PROCEDURE from <USER/ROLE>;
```

8.39 Limiting users by restricting the BECOME USER privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `BECOME USER` privilege allows the designated user to inherit the rights of another user.

Rationale:

As assignment of the `BECOME USER` privilege can allow the unauthorized use of another user's privileges, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='BECOME USER';
```

Remediation:

```
REVOKE BECOME USER from <USER/ROLE>;
```

8.40 Limiting users by restricting the SELECT ANY TABLE privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SELECT ANY TABLE` privilege allows the designated user to open any table to view it.

Rationale:

As assignment of the `SELECT ANY TABLE` privilege can allow the unauthorized viewing of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='SELECT_ANY_TABLE' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE SELECT_ANY_TABLE from <USER/ROLE>;
```

8.41 Limiting users by restricting the SELECT ANY DICTIONARY privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `SELECT ANY DICTIONARY` privilege allows the designated user to access SYS schema objects.

Rationale:

As assignment of the `SELECT ANY DICTIONARY` privilege can allow the unauthorized viewing of sensitive data, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='$SELECT_ANY_DICTIONARY' and USER not in
('SYS', 'SYSTEM');
```

Remediation:

```
REVOKE SELECT_ANY_DICTIONARY from <USER/ROLE>;
```

8.42 Limiting users by restricting the AUDIT SYSTEM privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `AUDIT SYSTEM` privilege allows the change auditing activities on the system.

Rationale:

As assignment of the `AUDIT SYSTEM` privilege can allow the unauthorized alteration of system audit activities, disabling the creation of audit trails, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='AUDIT SYSTEM' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE AUDIT SYSTEM from <USER/ROLE>;
```

8.43 Limiting users by restricting the AUDIT SYSTEM privilege (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `AUDIT SYSTEM` privilege allows the change auditing activities on the system.

Rationale:

As assignment of the `AUDIT SYSTEM` privilege can allow the unauthorized alteration of system audit activities, disabling the creation of audit trails, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_SYS_PRIVS where PRIVILEGE='AUDIT SYSTEM' and USER not in ('SYS',
'SYSTEM');
```

Remediation:

```
REVOKE AUDIT SYSTEM from <USER/ROLE>;
```

8.44 Limiting users by restricting privileges on PUBLIC (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `PUBLIC` user privileges are granted to all users that connect successfully to the database instance.

Rationale:

As assignment of any privileges to `PUBLIC` can provide an ingress point for unauthorized attempts to manipulate the system, these capabilities should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_ROLE_PRIVS where GRANTED_ROLE='PUBLIC';
```

Remediation:

```
REVOKE PUBLIC from <USER/ROLE>;
```

8.45 Limiting users by restricting the RESOURCE role (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `RESOURCE` role provides the user the `CREATE CLUSTER`, `CREATE INDEXTYPE`, `CREATE OPERATOR`, `CREATE PROCEDURE`, `CREATE SEQUENCE`, `CREATE TABLE`, `CREATE TRIGGER`, `CREATE TYPE` capabilities and is for compatibility with previous releases of Oracle Database.

Rationale:

As assignment of the `RESOURCE` role to a user can provide a great number of unnecessary privileges to ordinary users, application of this role should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_ROLE_PRIVS where GRANTED_ROLE='RESOURCE';
```

Remediation:

```
REVOKE RESOURCE from <USER/ROLE>;
```

8.46 Limiting users by restricting the DBA role (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBA` role is a "sample" database administrator role provided for the allocation of administrative privileges.

Rationale:

As assignment of the `DBA` role to a user can provide a great number of unnecessary privileges to ordinary users and opens the door to data breaches, integrity violations, and Denial-of-Service conditions, application of this role should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_ROLE_PRIVS where GRANTED_ROLE='DBA';
```

Remediation:

```
REVOKE RESOURCE from <USER/ROLE>;
```

8.47 Limiting user access to the UTL_FILE package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `UTL_FILE` package can be used to read/write file located on the server where the Oracle instance is installed.

Rationale:

As use of the `UTL_FILE` package could allow an unauthorized user to corrupt operating system files on the instance's host, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_FILE';
```

Remediation:

```
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
```

8.48 Limiting user access to the UTL_TCP package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `UTL_TCP` package can be used to read/write file to TCP sockets on the server where the Oracle instance is installed.

Rationale:

As use of the `UTL_TCP` package could allow an unauthorized user to corrupt the TCP stream used for carry the protocols that communicate with the instance's external

communications, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_TCP';
```

Remediation:

```
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
```

8.49 Limiting user access to the UTL_HTTP package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `UTL_HTTP` package can be used to read/write file to web-based applications on the server where the Oracle instance is installed.

Rationale:

As use of the `UTL_HTTP` package could allow an unauthorized user to corrupt the HTTP stream used for carry the protocols that communicate with the instance's web-based external communications, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_HTTP';
```

Remediation:

```
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
```

8.50 Limiting user access to the UTL_SMTP package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `UTL_SMTP` package can be used to send email from the server where the Oracle instance is installed.

Rationale:

As use of the `UTL_SMTP` package could allow an unauthorized user to corrupt the SMTP function to accept or generate junk mail that can result in a Denial-of-Service condition due to network saturation, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_SMTP';
```

Remediation:

```
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
```

8.51 Limiting user access to the DBMS_LOB package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBMS_LOB` package provides subprograms that can manipulate and read/write on BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs.

Rationale:

As use of the `DBMS_LOB` package could allow an unauthorized user to manipulate BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs on the instance, either destroying data or causing a Denial-of-Service condition due to corruption of disk space, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_LOB';
```

Remediation:

```
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
```

8.52 Limiting user access to the DBMS_SYS_SQL package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBMS_SYS_SQL` package is shipped as undocumented and is used for replication and other products such as WebDB, providing cursor access as the user..

Rationale:

As use of the `DBMS_SYS_SQL` package could allow an unauthorized user to access the cursor during a operations, effectively gaining whatever user privileges are associated with it, use of this package should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_SYS_SQL';
```

Remediation:

```
REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;
```

8.53 Limiting user access to the DBMS_JOB package (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBMS_JOB` package schedules and manages the jobs sent to the job queue and has been superseded by the `DBMS_SCHEDULER` package.

Rationale:

As use of the `DBMS_JOB` package could allow an unauthorized user to disable or overload the job queue and has been superseded by the `DBMS_SCHEDULER` package, this package should be disabled/restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_SYS_SQL';
```

Remediation:

```
REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;
```

8.54 Limiting user access to PROXY ACCOUNT authentication (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `PROXY ACCOUNT` user is an account that allows an authenticated connection "on behalf of" another user's account (e.g. Scott) to open a session. This allows a connection without the one requesting a proxy connection having to know Scott's password.

Rationale:

As use of the `PROXY ACCOUNT` authentication could allow an unauthorized user to gain access to the underlying privileges of the user allowing the proxy connection, this capability should be limited according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_TAB_PRIVS where GRANTEE='<PROXY ACCOUNT>'
SELECT * FROM DBA_ROLE_PRIVS where GRANTEE='<PROXY ACCOUNT>'
SELECT * FROM DBA_SYS_PRIVS where GRANTEE='<PROXY ACCOUNT>'
```

Remediation:

```
REVOKE ALL ON <USER>;
GRANT CREATE SESSION ON <USER>;
```

8.55 Limit public access to views beginning with ALL_ (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `ALL_` prefix allows the designated user to view the totality of the database objects attached to the prefix.

Rationale:

As assignment of the ALL_ prefix can allow access to view any object and potentially compromise database confidentiality/integrity, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE ('ALL_%') AND
GRANTEE='PUBLIC';
```

Remediation:

```
REVOKE ALL ON ALL_<NAME> from PUBLIC;
```

8.56 Limit public access to the DBMS_BACKUP_RESTORE (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database DBMS_BACKUP_RESTORE package is used for applying PL/SQL commands to the native RMAN sequences.

Rationale:

As assignment of use of the DBMS_BACKUP_RESTORE package can allow RMAN backup commands via PL/SQL and potentially compromise database backup media/operations, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_BACKUP_RESTORE'
```

Remediation:

```
REVOKE EXECUTE ON DBMS_BACKUP_RESTORE TO PUBLIC;
```

8.57 Limit public access to the DBMS_RANDOM (Scored)

Profile Applicability:

- Level 1

Description:

The Oracle database `DBMS_RANDOM` package is used for generating random numbers but should not be used for cryptographic purposes.

Rationale:

As assignment of use of the `DBMS_RANDOM` package can allow the unauthorized application of the random number-generating function, this capability should be restricted according to the needs of the organization.

Audit:

```
SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_RANDOM'
```

Remediation:

```
REVOKE EXECUTE ON DBMS_BACKUP_RESTORE TO PUBLIC;
REVOKE EXECUTE ON DBMS_BACKUP_RESTORE TO <USER>;
```

8.58 Limit access to standard database roles (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

The Oracle database `roles` are used for assigning one or more privileges or roles together administer user privileges on the database.

Rationale:

As the inappropriate assignment of user roles can allow unauthorized access to confidential information or violate database integrity, these capabilities should be restricted according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_ROLES;
```

Remediation:

```
SET ROLE <ROLE NAME> IDENTIFIED BY <PASSWORD>
```

9 General Policies and Procedures

There are number of general policies that cross multiple database environments or platform tiers and would have a significant impact on the instance and system's security profile.

9.1 Prohibit the database accessing a Public network interface card (Scored)

Profile Applicability:

- Level 1

Description:

Directly accessible public Network Interface Cards (NIC) allow any Internet-based user to attempt connection access to database services , such as the Listener, through the standard ports, e.g. 1521.

Rationale:

As having the database services directly accessible from the Internets without a firewall filter and private IP addressing can facilitate unauthorized connections, which at minimum would lead to Denial-of-Service attacks, IP addressing on the database host should be restricted according to the needs of the organization.

Audit:

```
Script to test for ip addresses other than 10.0.0.0-10.255.255.255, 172.16.0.0-
172.31.255.255, and 192.168.0.0-192.168.255.255
```

Remediation:

```
Use ipconfig tool to set script to a private ip address range
```

9.2 Permissions for database creation scripts (Scored)

Profile Applicability:

- Level 1

Description:

When creating an Oracle database and its configuration elements, the user is given the options to either save the creation script, a `CREATE DATABASE` statement that is a SQL statement to be run as a temple, or run the setup immediately.

Rationale:

As having the database template SQL scripts, for example "prod_db.sql," accessible by unauthorized users can facilitate attacks against the database data dictionary and structure, access to these templates should be restricted according to the needs of the organization.

Audit:

```
Check for permissions on:

C:\app\oracle\product\11.2.0\dbhome_1\rdbms\admin\dbname.sql
```

Remediation:

```
Set r/w permissions to be limited to the SYSTEM and DBA users.
```

9.3 Limit membership in the DBA users group (Scored)

Profile Applicability:

- Level 1

Description:

During the creation of an Oracle database and its data dictionary/connections, the most powerful database users are the default machine users SYS and SYSTEM. SYS can connect "as SYSDBA," taking on a role as with the same level of privileges as "root" in Unix" or "administrator" in Windows, making this user/role combination arguably the most powerful on the system. The "human" users who need to function as database administrators can be granted the "DBA" role, which contains by default all database system privileges and must have at least one user; these DBA privileges can also be subdivided and granted to new administrative DBA roles with fewer privileges, as well as having security administrators and network administrators.

Rationale:

As having the database's default DBA role assigned to all database administrators can lead to unintentional (and otherwise) access/damage to the instance, its data dictionary, and the data content, the full DBA role should subdivided among multiple administrators or be otherwise restricted according to the needs of the organization.

Audit:

```
Check for membership in the Windows DBA group
```

Remediation:

```
Remove all possible human users from the default DBA group.
```

9.4 Remove the username "oracle" from software account ownership (Scored)

Profile Applicability:

- Level 1

Description:

During the creation of an Oracle database the username "oracle" is the default name assigned to the ownership of the Oracle software account.

Rationale:

As leaving the database's default account name value as the well-know value "oracle" can facilitate attacks by unauthorized users, this username should be set according to the needs of the organization.

Audit:

```
Check for the name "oracle" among the Windows users
```

Remediation:

```
Change the ownership of software account value to other than "oracle"
```

10 Audit/Logging Policies and Procedures

The ability to audit system logs, to determine the result of user actions that have potentially resulted in the loss or violations of availability, confidentiality, and/or integrity is among the most important of all database security features. Decisions must be made regarding the breadth/depth of the logging activity, as greater detail produces larger log files. Measures must also be taken to protect the log files themselves, for these may be targeted for alteration or destruction to hide unauthorized activity. There are numerous command sequences for AUDIT, some of which are applicable to most database objects, such as CREATE, ALTER, DROP, while others are limited to a few database objects, such as GRANT,TRUNCATE,SET,SYSTEM AUDIT, and SYSTEM GRANT. The commands that apply to

larger numbers of objects will be addressed object by object after the primary connection commands are dealt with.

10.1 Audit all CREATE SESSION (logon/logoff) activities (Scored)

Profile Applicability:

- Level 1

Description:

The logging of all `CREATE SESSION` activities, the logon/logoff equivalent to remote database access , will provide an audit trail of user connection; this is the minimum privilege required to request access to run operations against the database.

Rationale:

As the logging of user connections to the database via logon/logoff activity can provide forensic evidence of the initiation of a pattern of unauthorized activities, this capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
SESSION';
```

Remediation:

```
AUDIT CREATE SESSION;
```

10.2 Audit all user CLUSTER activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `CLUSTER` privilege provides for the creation of interconnected computers/servers that appear as if they are one, increasing resource availability for a single instance.

Rationale:

As the logging of user connections to the database for the purpose of the creation, alteration, dropping , or truncation of a `CLUSTER` can provide forensic evidence of the

initiation of a pattern of unauthorized activities, this capability should be audited according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
CLUSTER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
CLUSTER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP ANY
CLUSTER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='TRUNCATE
CLUSTER';
```

Remediation:

```
AUDIT CLUSTER BY ACCESS;
AUDIT ALTER ANY CLUSTER BY ACCESS;
AUDIT DROP ANY CLUSTER BY ACCESS;
AUDIT TRUNCATE ANY CLUSTER BY ACCESS;
```

10.3 Audit all user CONTEXT activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `CONTEXT` object allows for the creation of a set of application-defined attributes that can validate and/or secure a specific application.

Rationale:

As the logging of user activities involving the creation, replacement, or dropping of a `CONTEXT` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
AUDIT CONTEXT BY ACCESS WHENEVER NOT SUCCESSFUL;
```

Remediation:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
CONTEXT'
```

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
CONTEXT'
```

10.4 Audit all user DATABASE LINK activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `DATABASE LINK` object allows for the creation of a link, either private or public, from an application-based "user" to the database for connections/session creation.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `DATABASE LINK` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
DATABASE LINK';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
DATABASE LINK';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
DATABASE LINK';
```

Remediation:

```
AUDIT DATABASE LINK BY ACCESS;
```

10.5 Audit all user SELECT ANY DICTIONARY activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `SELECT ANY DICTIONARY` capability allows the user to view the definitions of all schema objects in the database.

Rationale:

As the logging of user activities involving the capability to access the description of all schema objects in the database can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='SELECT ANY DICTIONARY';
```

Remediation:

```
AUDIT SELECT ANY DICTIONARY BY ACCESS;
```

10.6 Audit all user DIMENSION activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `DIMENSION` defines a parent-child relationship between pairs of column sets, where all of the columns of a given column set must come from the same table, but can be the source columns can come from different tables.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `DIMENSION` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
DIMENSION';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
DIMENSION';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
DIMENSION';
```

Remediation:

```
AUDIT DIMENSION BY ACCESS;
```

10.7 Audit all user DIRECTORY activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `DIRECTORY` object allows for the creation of a directory object that specifies an alias for a directory on the server file system, where the external binary file LOBs (BFILEs)/ table data are located.

Rationale:

As the logging of user activities involving the creation or dropping of a `DIRECTORY` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
DIRECTORY'
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
DIRECTORY'
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='GRANT
DIRECTORY'
```

Remediation:

```
AUDIT DIRECTORY BY ACCESS;
AUDIT GRANT DIRECTORY BY ACCESS;
```

10.8 Audit all user INDEX activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The INDEX object allows for the creation of a column (or columns) that reference data in a given data table, to increase the speed of data retrieval.

Rationale:

As the logging of user activities involving the creation, alter, or replacement of an INDEX can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
INDEX';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
INDEX';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
INDEX';
```

Remediation:

```
AUDIT CREATE ANY INDEX BY ACCESS;
AUDIT ALTER ANY INDEX BY ACCESS;
AUDIT DROP ANY INDEX BY ACCESS;
```

10.9 Audit all user MATERIALIZED VIEW activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `MATERIALIZED VIEW` object allows for the creation of a "Materialized view," which is a database object that can consist of the results gleaned from a query against data tables, views, or other materialized views.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `MATERIALIZED VIEW` can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
MATERIALIZED VIEW';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
MATERIALIZED VIEW';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
MATERIALIZED VIEW';
```

Remediation:

```
AUDIT CREATE ANY MATERIALIZED VIEW BY ACCESS;
AUDIT ALTER ANY MATERIALIZED VIEW BY ACCESS;
AUDIT DROP ANY MATERIALIZED VIEW BY ACCESS;
```

10.10 Audit all user GRANT ANY OBJECT PRIVILEGE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `GRANT ANY OBJECT PRIVILEGE` allows for the granting of any `OBJECT` privilege, which includes directories, flashbacks, mining models, etc.

Rationale:

As the logging of privilege grants that can lead to the creation, alteration, or dropping of tables, users and other critical system components is critical to forensic investigations, this audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE PRIVILEGE='GRANT ANY
OBJECT PRIVILEGE';
```

Remediation:

```
AUDIT GRANT ANY OBJECT PRIVILEGE BY ACCESS;
```

10.11 Audit all user GRANT ANY PRIVILEGE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `GRANT ANY PRIVILEGE` allows for the granting of any privilege, including those at the DBA level, so that the entire range of DBA capabilities is open to to the grantee.

Rationale:

As the logging of privilege grants that can lead to the creation, alteration, or dropping of tables, users and other critical system components, this audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE PRIVILEGE='GRANT ANY
PRIVILEGE';
```

Remediation:

```
AUDIT GRANT ANY PRIVILEGE BY ACCESS;
```

10.12 Audit all user PROCEDURE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `AUDIT PROCEDURE` audit command allows for the tracking a number of user activities, including the:

`FUNCTION`, the creation/dropping of a standalone stored function or a "Call specification" that is like a procedure, except functions return values to its original environment and can be in Java or other 3GL languages;

`LIBRARY`, the creation/dropping of a schema object associated with an operating-system shared library;

`PACKAGE`, the creation/dropping of a locally stored collection of related procedures, functions, and potentially other program objects stored together; and

`PROCEDURE`, the creation/dropping of a procedure, which is a subprogram that performs a specified action and is stored in the database.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `PROCEDURE` and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
FUNCTION';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
FUNCTION';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
ANY LIBRARY';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
LIBRARY';
```

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
PACKAGE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
PACKAGE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
PROCEDURE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
PROCEDURE';
```

Remediation:

AUDIT CREATE PROCEDURE BY ACCESS;

```
AUDIT ALTER ANY PROCEDURE BY ACCESS;
AUDIT DROP ANY PROCEDURE BY ACCESS;
AUDIT EXECUTE ANY PROCEDURE WHENEVER NOT SUCCESSFUL;
AUDIT CREATE ANY LIBRARY BY ACCESS;
AUDIT DROP ANY LIBRARY BY ACCESS;
```

10.13 Audit all user PROFILE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `PROFILE` object allows for the creation of a set of database resource limits that can be assigned to a user, so that that user cannot exceed those resource limitations.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `PROFILE` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
PROFILE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
PROFILE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
PROFILE;
```

Remediation:

```
AUDIT CREATE PROFILE BY ACCESS;
AUDIT ALTER PROFILE BY ACCESS;
AUDIT DROP PROFILE BY ACCESS;
```

10.14 Audit all user PUBLIC DATABASE LINK activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `PUBLIC DATABASE LINK` object allows for the creation of a public link for an application-based "user" to access the database for connections/session creation .

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `PUBLIC DATABASE LINK` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
PUBLIC DATABASE LINK';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
PUBLIC DATABASE LINK';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
PUBLIC DATABASE LINK';
```

Remediation:

```
AUDIT CREATE PUBLIC DATABASE LINK BY ACCESS;
AUDIT ALTER PUBLIC DATABASE LINK BY ACCESS;
AUDIT DROP PUBLIC DATABASE LINK BY ACCESS;
```

10.15 Audit all user PUBLIC SYNONYM activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `PUBLIC SYNONYM` object allows for the creation of an alternate description of an object and public synonyms are accessible by all users that have the appropriate privileges to the underlying object.

Rationale:

As the logging of user activities involving the creation or dropping of a PUBLIC SYNONYM can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
PUBLIC SYNONYM';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
PUBLIC SYNONYM';
```

Remediation:

```
AUDIT CREATE PUBLIC SYNONYM BY ACCESS;
AUDIT DROP PUBLIC SYNONYM BY ACCESS;
```

10.16 Audit all user ROLE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The ROLE object allows for the creation of a set of privileges that can be granted to users/ other roles, both for application connection and database administrative purposes.

Rationale:

As the logging of user activities involving the creation, alteration, setting or dropping of a ROLE can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
ROLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
ROLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='SET
ROLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
ROLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
ROLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='GRANT ANY
ROLE';
```

Remediation:

```
AUDIT CREATE ROLE BY ACCESS;
AUDIT ALTER ANY ROLE BY ACCESS;
AUDIT DROP ANY ROLE BY ACCESS;
AUDIT GRANT ANY ROLE BY ACCESS;
```

10.17 Audit all user ROLLBACK SEGMENT activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `ROLLBACK SEGMENT` object allows for the creation of an object that the Oracle Database will use to store whatever data is required to undo, changes made by prior transactions.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `ROLLBACK SEGMENT` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
ROLLBACK SEGMENT';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
ROLLBACK SEGMENT';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
ROLLBACK SEGMENT';
```

Remediation:

```
AUDIT CREATE ROLLBACK SEGMENT BY ACCESS;
AUDIT ALTER ROLLBACK SEGMENT BY ACCESS;
AUDIT DROP ROLLBACK SEGMENT BY ACCESS;
```

10.18 Audit all user SEQUENCE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `SEQUENCE` operation allows for the creation of a database object that allows multiple users to generate unique integers that can be used to create primary key values automatically.

Rationale:

As the logging of user activities involving the creation or dropping of a `SEQUENCE` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
SEQUENCE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
SEQUENCE';
```

Remediation:

```
AUDIT SEQUENCE BY ACCESS WHENEVER NOT SUCCESSFUL;
```

10.19 Audit all user SYNONYOM activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `SYNONYM` operation allows for the creation of a an alternative name for a database object such as a Java class schema object, materialized view, operator, package, procedure, sequence, stored function, table, view, user-defined object type, even another synonym; this synonym puts a dependency on its target and is rendered invalid if the target object is changed/dropped.

Rationale:

As the logging of user activities involving the creation or dropping of a `SYNONYM` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
SYNONYM';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
SYNONYM';
```

Remediation:

```
AUDIT SYNONYM BY ACCESS;
```

10.20 Audit all user TABLE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `TABLE` object is the "base" of the relational database and holds user/schema data that is used as the source to create relationships between the data inside. (This data can be stored as alphanumeric or binary.)

Rationale:

As the logging of user activities involving the creation, truncation, or dropping of a `TABLE` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
TABLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='TRUNCATE
TABLE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP ANY
TABLE';
```

Remediation:

```
AUDIT TABLE BY ACCESS;
```

10.21 Audit all user TABLESPACE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `TABLESPACE` object is a *logical* unit that holds indexes and/or tables of user/schema data in a *physical* location on a disk. The tablespace functions as the bridge or connection between the database itself and the physical filesystem which hold's the table(s) or index(es).

Rationale:

As the logging of user activities involving the creation, truncation, or dropping of a `TABLESPACE` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
TABLESPACE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='TRUNCATE
TABLESPACE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
TABLESPACE';
```

Remediation:

```
AUDIT TABLESPACE BY ACCESS;
AUDIT CREATE TABLESPACE BY ACCESS;
AUDIT DROP TABLESPACE BY ACCESS;
```

10.22 Audit all user TRIGGER activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `TRIGGER` object for the Oracle database is analogous to an "if/then' condition in computer code; these procedures are stored in the database and will run if a certain condition is met or an event occurs.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `TRIGGER` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
TRIGGER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
TRIGGER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
TRIGGER';
```

Remediation:

```
AUDIT CREATE ANY TRIGGER BY ACCESS;
AUDIT ALTER ANY TRIGGER BY ACCESS;
```

```
AUDIT DROP ANY TRIGGER BY ACCESS;
```

10.23 Audit all user TYPE activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `TYPE` object for the Oracle database is specifications of an object type, which can be a SQLJ object type, a named varying array (varray), a nested table type, object reference types, or even an incomplete object type.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `TYPE` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
TYPE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
TYPE BODY';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
TYPE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
TYPE';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP TYPE
BODY';
```

Remediation:

```
AUDIT CREATE ANY TYPE BY ACCESS;
AUDIT ALTER ANY TYPE BY ACCESS;
```

```
AUDIT DROP ANY TYPE BY ACCESS;
```

10.24 Audit all USER object activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `USER` object for the Oracle database is a specification of an object which is an account through which either a human or an application can connect to, via a JDBC or log into, via a CLI, and interact with the database instance according to the roles and privileges allotted to account.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `USER` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
USER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
USER';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
USER';
```

Remediation:

```
AUDIT CREATE USER BY ACCESS;
AUDIT ALTER USER BY ACCESS;
AUDIT DROP USER BY ACCESS;
```

10.25 Audit all VIEW object activities/requests (Scored)

Profile Applicability:

- Level 1

Description:

The `VIEW` object for the Oracle database is a logical table that has been created from a compilation of one or more base tables or views, which is equal in sensitivity to the source data, but still contains no original data, only that has come from its input sources.

Rationale:

As the logging of user activities involving the creation, alteration, or dropping of a `VIEW` can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

Audit:

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='CREATE
VIEW';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='ALTER
VIEW';
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
VIEW';
```

Remediation:

```
AUDIT CREATE VIEW BY ACCESS;
AUDIT ALTER VIEW BY ACCESS;
AUDIT DROP VIEW BY ACCESS;
```

10.26 Audit all unsuccessful table SELECT activities (Scored)

Profile Applicability:

- Level 1

Description:

The logging of unsuccessful attempts to `SELECT` (open for read/update/delete/view) various tables audit will provide an audit trail of user connection activities that may indicate unauthorized attempts to access the data tables.

Rationale:

As the logging of unsuccessful attempts to initiate a `SELECT` command can provide forensic evidence of the initiation of a pattern of unauthorized activities, this logging capability should be set according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME='<OBJECT_NAME>';
```

Remediation:

```
AUDIT SELECT ON TABLE WHENEVER NOT SUCCESSFUL
```

10.27 Audit all SELECT ANY TRANSACTION activities (Scored)

Profile Applicability:

- Level 1

Description:

The logging of all `SELECT ANY TRANSACTION` (open for read/ view) shows the contents of the `FLASHBACK_TRANSACTION_QUERY` view, which can view all data in the database, including past data.

Rationale:

As the logging of `SELECT ANY TRANSACTION` command can provide forensic evidence on the initiation of a pattern of unauthorized activities, this logging capability should be set according to the needs of the organization.

Audit:

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME='< SELECT ANY TRANSACTION >';
```

Remediation:

```
AUDIT SELECT ANY TRANSACTION;
```

10.28 Set AUDIT ALL ON SYS.AUD$ activities (Scored)

Profile Applicability:

- Level 1

Description:

The logging of attempts to alter the audit trail in the `SYS.AUD$` table (open for read/update/delete/view) will provide a record of any activities that may indicate unauthorized attempts to access the audit trail.

Rationale:

As the logging of attempts to alter the `SYS.AUD$` table can provide forensic evidence of the initiation of a pattern of unauthorized activities, this logging capability should be set according to the needs of the organization.

Audit:

```
SELECT * from DBA_OBJ_AUDIT_OPTS where OBJECT_NAME='AUD$';
```

Remediation:

```
AUDIT ALL on SYS.AUD$ BY ACCESS;
```

Appendix: Change History

Date	Version	Changes for this version
11-15-2012	1.0.0	Initial release.