

Oracle Database Management System Security Standard

Oracle Database Management System Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies technical security policy for implementations of Oracle and applies to Oracle implementations 8.0 and above.

This standard contains 67 baseline controls, and 2 above baseline controls, for a total of 69 controls.

Important

All of these Security Standards and Security Policies are copyrighted. THEY ARE NOT IN THE PUBLIC DOMAIN. They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

Table of Contents

1. Introduction	1
1.1. Objectives	1
1.2. Scope	1
1.3. Not In Scope	1
1.4. Giving Feedback	1
1.5. Publishing these Security Standards and Policies	1
1.6. Related Documents	2
1.6.1. Generic Security Standards	2
1.6.2. Operating System Security Standards	2
1.6.3. Database Security Standards	3
1.7. Definitions	3
2. User Configuration	4
2.1. User Administration	4
2.1.1. User profile names on the database should be consistent with their other login names	4
2.1.2. Accounts belonging to personnel who have fixed periods of employments should be set up with expiration dates	4
2.1.3. Scripted modifications to users should use up to date commands	5
2.1.4. Database administrators should perform periodic user account audits	6
2.2. Default Accounts	6
2.2.1. The default password for the demo account should be changed	6
2.2.2. The default password for the dbsnmp account should be changed	7
2.2.3. The default password for the scott account should be changed	8
2.2.4. The default password for the p08 account should be changed	8
2.2.5. The default password for the system account should be changed	9
2.2.6. The default password for the sys account should be changed	10
2.2.7. The scott account should be deleted if possible	10
2.3. Roles, Views, and Access Control	11
2.3.1. Users with a requirement for a single role should be denied the ability to execute the set role command	11
2.3.2. Access to the operating system command line interface should be denied from users where possible.	11
2.3.3. Password protected roles should be implemented.	12
2.3.4. Views should be used to enforce access restrictions to tables.	13
2.3.5. Users must not be assigned any default Oracle roles	13
2.3.6. For live database apps do not use the connect or resource roles	14
2.3.7. Applications should be developed with password protected roles without hard-coding the role password or disclosing the role password to the users	14
2.3.8. Database views should be defined that map to database roles	15
2.4. Privileges	16
2.4.1. The CREATE privilege should not be granted to any application.	16
2.4.2. The DROP privilege should not be granted to any application.	16
2.4.3. The DBA role must be granted to Database Administrators alone	17
2.4.4. The UNLIMITED TABLESPACE privilege should not be granted to any application.	18
2.4.5. The EXECUTE ANY PROCEDURE privilege should not be granted to any application.	18
2.4.6. If the scott account exists, it should have the CONNECT privilege only	19
2.4.7. Privileges should be assigned to roles and not directly to users	19
2.4.8. The ALTER privilege should not be granted to any application.	20
2.4.9. The BECOME USER privilege should not be granted to any application.	20
2.4.10. The GRANT ANY PRIVILEGE/ROLE privilege should not be granted to any application.	21

2.4.11. The p08 account should have the DBA role revoked	22
2.5. Authentication/Password Configuration	22
2.5.1. Sessions per user should be restricted to 1	22
2.5.2. Password reuse max should be set to 12 passwords	23
2.5.3. Password lifetime should be set to 30 days	24
2.5.4. Account logins should timeout and disconnect after 30 minutes of inactivity	24
2.5.5. Password grace time should be set to 0 days	25
2.5.6. Password lock time should be set to maximum possible time	25
2.5.7. User accounts must not be set such that the user cannot change their password	26
2.5.8. User account passwords must contain at least one numeric character	27
2.5.9. Accounts must have a password minimum length of 6 characters	27
3. Network Security Configuration	29
3.1. Network Interface Considerations	29
3.1.1. The listener.ora file should be readable only by the administrators	29
3.1.2. Use Advanced Networking Option to provide encrypted data transfer	29
3.1.3. Oracle passwords should be protected from traversing the network in clear text.	30
3.1.4. Network listeners for SQL*NET clients should be password protected	31
3.1.5. The passwords for the listeners for SQL*NET clients should be changed from the default value	31
4. Configuration	33
4.1. Files and File Permissions	33
4.1.1. The config.ora file should be afforded the same control as the init.ora object	33
4.1.2. The object CATALOG.BSQ must not be modified	33
4.1.3. The object SQL.BSQ must not be modified	34
4.1.4. All Oracle database control files should have consistent permission masks ...	34
4.1.5. The owner of the database files should be Oracle	35
4.1.6. Oracle users must not have greater access to the database files than that set by the Oracle installation	36
4.1.7. The database control file must be owned by Oracle	36
4.1.8. When assigning user rights to an object never use Grant All	37
4.1.9. Database files should be protected from unauthorised access	37
4.1.10. The Oracle database initialisation file should be available to the Oracle system account alone	38
4.1.11. The Oracle database initialisation file must not be user readable	38
4.2. Administration	39
4.2.1. The use of quotas should be considered	39
4.2.2. Maintain version control and change comments in the Oracle initialisation file	40
4.2.3. Check users privileges following an upgrade	40
4.2.4. If using Oracle Enterprise Manager ensure the workstations/consoles on which it is run are protected from attack.	41
4.3. Backups	42
4.3.1. Online image backups should be taken	42
4.3.2. Online incremental backups should be taken	42
5. Auditing and Monitoring	44
5.1. Events to be alerted in real-time	44
5.1.1. The system resource profile settings for password lock time should be set to forever	44
5.1.2. User accounts should be locked out after 3 consecutive login failures	44
5.2. Events to be audited	45
5.2.1. Enable auditing	45
5.2.2. The init.ora file must be modified for data dictionary auditing to be enabled.	47
5.2.3. Use triggers to capture audit information where it is not captured in table information	48
5.2.4. Use triggers to log modifications to the DBA_USERS table	49
5.2.5. Tables should be designed to include extra fields for auditing actions taken .	49

6. Other	51
6.1. When an object is deleted from the database, delete all related synonyms	51
6.1.1. Standard	51
6.1.2. Detailed Steps	51
6.1.3. Risks Addressed	51
7. Checklist	52

Chapter 1. Introduction

1.1. Objectives

The objectives of this document are:

- To specify a baseline configuration for implementations of <trademark>Oracle</trademark> RDBMS
- To provide guidance to administrators, developers and security personnel in securely implementing <trademark>Oracle</trademark> Database Management System.

1.2. Scope

Controls specified in this document apply to Oracle implementations 8.0 and above.

All of the organisation's Oracle implementations will be subject to the policies specified within this security standard. The policies will be applied to new and existing installations.

1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from your Information Security team consultancy function.

This is a specific standard for Oracle RDBMS 8.0 and above. Other Oracle products are subjected to separate standards.

Compliance with this standard does not negate the need for an overall security review of a proposed application. Contact the Information Security team if you are in doubt.

1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.
- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

1.6.1. Generic Security Standards

Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

Data Protection European Union Security Standard

<http://www.frankodwyer.com/standards/index.html#generic>

Application Service Provider Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

1.6.2. Operating System Security Standards

Generic Unix Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Workstation Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Server Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Domain Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

1.6.3. Database Security Standards

Oracle Security Standards

<http://www.frankodwyer.com/standards/index.html#db>

1.7. Definitions

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, off the shelf software, hardware, media, data item, data item repository and associated communications networks. The specification of the Information Asset in question will usually be given so that this document is unambiguous.

Chapter 2. User Configuration

2.1. User Administration

2.1.1. User profile names on the database should be consistent with their other login names

ID	Version	Level	Enforcement
ORAC-UA-1	1.0	baseline	recommended

2.1.1.1. Standard

User profile names on the database should be consistent with their other login names

2.1.1.2. Detailed Steps

- Define security administration procedures that result in consistent user naming

2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Inconsistent user profile names may result in user ids not being removed when a user transfers or leaves
- These unauthorised accounts may be used to compromise the system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.2. Accounts belonging to personnel who have fixed periods of employments should be set up with expiration dates

ID	Version	Level	Enforcement
ORAC-UA-4	1.0	baseline	recommended

2.1.2.1. Standard

Accounts belonging to personnel who have a fixed period of employment should be set up with expiration dates

2.1.2.2. Detailed Steps

- During the account request process obtain account expiration information.
- Set up the account with an expiration date

2.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Redundant accounts are often targeted for compromise
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.3. Scripted modifications to users should use up to date commands

ID	Version	Level	Enforcement
ORAC-ADMIN-10	1.0	baseline	recommended

2.1.3.1. Standard

Scripted modifications to users should use up to date commands

2.1.3.2. Detailed Steps

- Identify scripts that modify database users
- Ensure that "alter user" is used instead of older commands

2.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.4. Database administrators should perform periodic user account audits

ID	Version	Level	Enforcement
ORAC-UA-2	1.0	baseline	recommended

2.1.4.1. Standard

Database administrators should perform periodic user account audits to ensure access granted is still required.

2.1.4.2. Detailed Steps

- Produce a list of user profiles who have access to the DBMS
- Check that the level of access these accounts have with the application owner
- Remove any accounts no longer required
- Modify any account access that is no longer appropriate

2.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Redundant accounts can be targeted to gain unauthorised access
- Redundant access rights can be used to perform unauthorised actions
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2. Default Accounts

2.2.1. The default password for the demo account should be changed

ID	Version	Level	Enforcement
ORAC-DA-5	1.0	baseline	recommended

2.2.1.1. Standard

The default password for the demo account should be changed

2.2.1.2. Detailed Steps

- Change the default password for the demo account following installation

2.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.2. The default password for the dbsnmp account should be changed

ID	Version	Level	Enforcement
ORAC-DA-3	1.0	baseline	recommended

2.2.2.1. Standard

The default password for the dbsnmp account should be changed

2.2.2.2. Detailed Steps

- Change the default password for the dbsnmp account following installation

2.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.3. The default password for the scott account should be changed

ID	Version	Level	Enforcement
ORAC-DA-4	1.0	baseline	recommended

2.2.3.1. Standard

The default password for the scott account should be changed

2.2.3.2. Detailed Steps

- Change the default password for the scott account following installation

2.2.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.4. The default password for the p08 account should be changed

ID	Version	Level	Enforcement
ORAC-DA-6	1.0	baseline	recommended

2.2.4.1. Standard

The default password for the p08 account should be changed

2.2.4.2. Detailed Steps

- Change the default password for the p08 account following installation

2.2.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.5. The default password for the system account should be changed

ID	Version	Level	Enforcement
ORAC-DA-2	1.0	baseline	recommended

2.2.5.1. Standard

The default password for the sys account should be changed

2.2.5.2. Detailed Steps

- Change the default password for the system account following installation

2.2.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.6. The default password for the sys account should

be changed

ID	Version	Level	Enforcement
ORAC-DA-1	1.0	baseline	recommended

2.2.6.1. Standard

The default password for the sys account should be changed

2.2.6.2. Detailed Steps

- Change the default password for the sys account following installation

2.2.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.7. The scott account should be deleted if possible

ID	Version	Level	Enforcement
ORAC-DA-7	1.0	baseline	recommended

2.2.7.1. Standard

The scott account should be deleted if possible

2.2.7.2. Detailed Steps

- If possible delete the scott following installation.

2.2.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3. Roles, Views, and Access Control

2.3.1. Users with a requirement for a single role should be denied the ability to execute the set role command

ID	Version	Level	Enforcement
ORAC-ACC-8	1.0	baseline	recommended

2.3.1.1. Standard

Users with a requirement for a single role should be denied the ability to execute the set role command

2.3.1.2. Detailed Steps

- Deny users access to the DBMS command prompt

2.3.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to the CLI can be used to subvert the application security controls
- Access to the CLI can be used to subvert the database security controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.2. Access to the operating system command line interface should be denied from users where possible.

ID	Version	Level	Enforcement
ORAC-ACC-7	1.0	baseline	recommended

2.3.2.1. Standard

Access to the operating system command line interface should be denied from users where possible.

2.3.2.2. Detailed Steps

- Use the product_profile table to block the host command

2.3.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to the CLI can be used to subvert the application security controls
- Access to the CLI can be used to subvert the database security controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.3. Password protected roles should be implemented.

ID	Version	Level	Enforcement
ORAC-ACC-4	1.0	baseline	recommended

2.3.3.1. Standard

Password protected roles should be implemented.

2.3.3.2. Detailed Steps

- Password protect roles on the database

2.3.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.4. Views should be used to enforce access restrictions to tables.

ID	Version	Level	Enforcement
ORAC-ACC-1	1.0	baseline	recommended

2.3.4.1. Standard

Views should be used to enforce access restrictions to tables.

2.3.4.2. Detailed Steps

- Define the data access requirement each role needs to have for the database
- Define views according to these role access requirements

2.3.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Inconsistent access control allows application restrictions to be bypassed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.5. Users must not be assigned any default Oracle roles

ID	Version	Level	Enforcement
ORAC-ACC-3	1.0	baseline	mandatory

2.3.5.1. Standard

Users must not be assigned any default Oracle roles

2.3.5.2. Detailed Steps

- Remove any default roles from the Oracle users
- Assign the users appropriate created roles

- Ensure the created roles only have CREATE SESSION privilege

2.3.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Default roles may provide unintended access to the database
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.6. For live database apps do not use the connect or resource roles

ID	Version	Level	Enforcement
ORAC-ACC-6	1.0	baseline	recommended

2.3.6.1. Standard

For live database apps do not use the connect or resource roles

2.3.6.2. Detailed Steps

- Do not assign the connect or resource roles to any users

2.3.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.7. Applications should be developed with password protected roles without hard-coding the role password or disclosing the role password to the users

ID	Version	Level	Enforcement
ORAC-ACC-5	1.0	baseline	recommended

2.3.7.1. Standard

Applications should be developed with password protected roles without hard-coding the role password or disclosing the role password to the users

2.3.7.2. Detailed Steps

- Password protect roles on the database
- Do not hard code the password into the application
- Do not disclose the role password to the users
- Make the role a default role for the user

2.3.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.8. Database views should be defined that map to database roles

ID	Version	Level	Enforcement
ORAC-ACC-2	1.0	baseline	recommended

2.3.8.1. Standard

Database views should be defined that map to database roles

2.3.8.2. Detailed Steps

- Use the management interface to define roles
- Use the privilege management interface to define database views that map to the roles

2.3.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4. Privileges

2.4.1. The CREATE privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-6	1.0	baseline	recommended

2.4.1.1. Standard

The CREATE privilege should not be granted to any application.

2.4.1.2. Detailed Steps

- Ensure that applications are not granted the CREATE privilege.

2.4.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.2. The DROP privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-5	1.0	baseline	recommended

2.4.2.1. Standard

The DROP privilege should not be granted to any application.

2.4.2.2. Detailed Steps

- Ensure that applications are not granted the DROP privilege.

2.4.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.3. The DBA role must be granted to Database Administrators alone

ID	Version	Level	Enforcement
ORAC-PRIV-4	1.0	baseline	mandatory

2.4.3.1. Standard

The DBA role must be granted to Database Administrators alone

2.4.3.2. Detailed Steps

- Ensure that the only holders of the DBA role are Database Administrators

2.4.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised unrestricted privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.4. The UNLIMITED TABLESPACE privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-11	1.0	baseline	recommended

2.4.4.1. Standard

The UNLIMITED TABLESPACE privilege should not be granted to any application.

2.4.4.2. Detailed Steps

- Ensure that applications are not granted the UNLIMITED TABLESPACE privilege.

2.4.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.5. The EXECUTE ANY PROCEDURE privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-10	1.0	baseline	recommended

2.4.5.1. Standard

The EXECUTE ANY PROCEDURE privilege should not be granted to any application.

2.4.5.2. Detailed Steps

- Ensure that applications are not granted the EXECUTE ANY PROCEDURE privilege.

2.4.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.6. If the scott account exists, it should have the CONNECT privilege only

ID	Version	Level	Enforcement
ORAC-PRIV-1	1.0	baseline	recommended

2.4.6.1. Standard

If the scott account exists, it should have the CONNECT privilege only

2.4.6.2. Detailed Steps

- If the scott account exists, remove all privileges except CONNECT

2.4.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.7. Privileges should be assigned to roles and not directly to users

ID	Version	Level	Enforcement
ORAC-PRIV-12	1.0	baseline	recommended

2.4.7.1. Standard

Privileges should be assigned to roles and not directly to users

2.4.7.2. Detailed Steps

- Use the privilege management interface to define roles
- Use the privilege management interface to assign users to roles

2.4.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.8. The ALTER privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-7	1.0	baseline	recommended

2.4.8.1. Standard

The ALTER privilege should not be granted to any application.

2.4.8.2. Detailed Steps

- Ensure that applications are not granted the ALTER privilege.

2.4.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.9. The BECOME USER privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-8	1.0	baseline	recommended

2.4.9.1. Standard

The BECOME USER privilege should not be granted to any application.

2.4.9.2. Detailed Steps

- Ensure that applications are not granted the BECOME USER privilege.

2.4.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.10. The GRANT ANY PRIVILEGE/ROLE privilege should not be granted to any application.

ID	Version	Level	Enforcement
ORAC-PRIV-9	1.0	baseline	recommended

2.4.10.1. Standard

The GRANT ANY PRIVILEGE/ROLE privilege should not be granted to any application.

2.4.10.2. Detailed Steps

- Ensure that applications are not granted the GRANT ANY PRIVILEGE/ROLE privilege.

2.4.10.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.11. The p08 account should have the DBA role revoked

ID	Version	Level	Enforcement
ORAC-PRIV-2	1.0	baseline	recommended

2.4.11.1. Standard

The p08 account should have the DBA role revoked

2.4.11.2. Detailed Steps

- If the p08 exists, remove the DBA role.

2.4.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5. Authentication/Password Configuration

2.5.1. Sessions per user should be restricted to 1

ID	Version	Level	Enforcement
ORAC-AUTH-8	1.0	baseline	recommended

2.5.1.1. Standard

The number of concurrent sessions per user should be restricted to 1

2.5.1.2. Detailed Steps

- The system resource profile settings should be configured such that the sessions per user value is restricted to 1

2.5.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reduces the risk of account sharing
- Reduces the risk of compromised accounts going unnoticed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.2. Password reuse max should be set to 12 passwords

ID	Version	Level	Enforcement
ORAC-AUTH-7	1.0	baseline	recommended

2.5.2.1. Standard

The Password reuse max value should be set to 12 passwords to prevent the reuse of the previous 12 passwords used by an account holder

2.5.2.2. Detailed Steps

- The system resource profile settings should be configured such that the password reuse max value is set to 12 passwords.

2.5.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Reuse of passwords extends the effective password lifetime
- The greater the password lifetime the greater the risk of compromise
- The greater the password lifetime the greater the period within which a compromised password can be used
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.

- Business information and applications may be unavailable.

2.5.3. Password lifetime should be set to 30 days

ID	Version	Level	Enforcement
ORAC-AUTH-5	1.0	baseline	recommended

2.5.3.1. Standard

Password lifetime should be set to 30 days

2.5.3.2. Detailed Steps

- The system resource profile settings should be configured such that the password lifetime is set to 30 days.

2.5.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Long password lifetimes increases the opportunity for password exposure
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.4. Account logins should timeout and disconnect after 30 minutes of inactivity

ID	Version	Level	Enforcement
ORAC-AUTH-3	1.0	baseline	recommended

2.5.4.1. Standard

Account logins should timeout and disconnect after 30 minutes of inactivity

2.5.4.2. Detailed Steps

- The system resource profile settings should be configured to to timeout and disconnect account logins after 30 minutes of user inactivity

2.5.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Accounts logged in but inactive may be subject to unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.5. Password grace time should be set to 0 days

ID	Version	Level	Enforcement
ORAC-AUTH-4	1.0	baseline	recommended

2.5.5.1. Standard

Password grace time should be set to 0 days

2.5.5.2. Detailed Steps

- The system resource profile settings should be configured such that the password grace time is set to 0 days

2.5.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The password lifetime exists to enforce password change to limit the period of exposure that may exist should a password be compromised
- Password grace time extends the effective password lifetime and thus the period of time for potential exposure
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.6. Password lock time should be set to maximum possible time

ID	Version	Level	Enforcement
ORAC-AUTH-6	1.0	baseline	recommended

2.5.6.1. Standard

Password lock time should be set to maximum possible time

2.5.6.2. Detailed Steps

- The system resource profile settings should be configured such that the password lock time is set to the maximum possible value.

2.5.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Allowing potentially successful attempts to log in to an account after the login failure limit has been reached increases the likelihood of the account becoming compromised.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.7. User accounts must not be set such that the user cannot change their password

ID	Version	Level	Enforcement
ORAC-UA-3	1.0	baseline	mandatory

2.5.7.1. Standard

User accounts must not be set such that the user cannot change their password

2.5.7.2. Detailed Steps

- Select change password at next logon for the account in question

2.5.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Account passwords may be compromised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.8. User account passwords must contain at least one numeric character

ID	Version	Level	Enforcement
ORAC-AUTH-2	1.0	baseline	mandatory

2.5.8.1. Standard

User account passwords must contain at least one numeric character

2.5.8.2. Detailed Steps

- The password management system must be enabled
- The password complexity function must be set to ensure a minimum of 1 numeric character in the password

2.5.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Increasing password complexity makes passwords harder to guess
- Easily guessed passwords may result in compromise of accounts
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.9. Accounts must have a password minimum length of 6 characters

ID	Version	Level	Enforcement
ORAC-AUTH-1	1.0	baseline	mandatory

2.5.9.1. Standard

Accounts must have a password minimum length of 6 characters

2.5.9.2. Detailed Steps

- The password management system must be enabled
- The minimum length for passwords must be set to 6 characters

2.5.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Short passwords are easier to guess
- Easily guessed passwords may result in compromise of accounts
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 3. Network Security Configuration

3.1. Network Interface Considerations

3.1.1. The listener.ora file should be readable only by the administrators

ID	Version	Level	Enforcement
ORAC-NET-5	1.0	baseline	recommended

3.1.1.1. Standard

The listener.ora file should be readable only by the administrators

3.1.1.2. Detailed Steps

- Ensure the file ownership is not changed from installation time
- Ensure that the file permissions do not permit read access other than for the administrators

3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.2. Use Advanced Networking Option to provide encrypted data transfer

ID	Version	Level	Enforcement
ORAC-NET-1	1.0	above baseline	recommended

3.1.2.1. Standard

Use Advanced Networking Option to provide encrypted data transfer

3.1.2.2. Detailed Steps

- Install the ANO
- Configure ANO to encrypt data transmission from clients to servers for sensitive applications

3.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Data transmitted in clear text is subject to disclosure
- Data transmitted in clear text is subject to modification
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.3. Oracle passwords should be protected from traversing the network in clear text.

ID	Version	Level	Enforcement
ORAC-NET-2	1.0	above baseline	recommended

3.1.3.1. Standard

The advanced networking option should be implemented so as to protect Oracle passwords in transmission across the network.

3.1.3.2. Detailed Steps

- Install the ANO
- Configure ANO to encrypt passwords in transmission from clients to servers

3.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Passwords transmitted in clear text are subject to disclosure
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.4. Network listeners for SQL*NET clients should be password protected

ID	Version	Level	Enforcement
ORAC-NET-3	1.0	baseline	recommended

3.1.4.1. Standard

Network listeners for SQL*NET clients should be password protected

3.1.4.2. Detailed Steps

- Implement passwords on the SQL*NET listeners

3.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.5. The passwords for the listeners for SQL*NET clients should be changed from the default value

ID	Version	Level	Enforcement
ORAC-NET-4	1.0	baseline	recommended

3.1.5.1. Standard

The passwords for the listeners for SQL*NET clients should be changed from the default value

3.1.5.2. Detailed Steps

- Change the passwords on the SQL*NET listeners

3.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 4. Configuration

4.1. Files and File Permissions

4.1.1. The config.ora file should be afforded the same control as the init.ora object

ID	Version	Level	Enforcement
ORAC-FP-8	1.0	baseline	recommended

4.1.1.1. Standard

The config.ora file should be afforded the same control as the init.ora object

4.1.1.2. Detailed Steps

- Ensure that the ownership of config.ora is the same as that for init.ora
- Ensure that the file permissions of config.ora are the same as that for init.ora

4.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.2. The object CATALOG.BSQ must not be modified

ID	Version	Level	Enforcement
ORAC-FP-10	1.0	baseline	mandatory

4.1.2.1. Standard

The object CATALOG.BSQ must not be modified

4.1.2.2. Detailed Steps

- Ensure that the CATALOG.BSQ file permissions are set to prevent unauthorised modification

4.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.3. The object SQL.BSQ must not be modified

ID	Version	Level	Enforcement
ORAC-FP-9	1.0	baseline	mandatory

4.1.3.1. Standard

The object SQL.BSQ must not be modified

4.1.3.2. Detailed Steps

- Ensure that the SQL.BSQ file permissions are set to prevent unauthorised modification

4.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.4. All Oracle database control files should have consistent permission masks

ID	Version	Level	Enforcement
ORAC-FP-5	1.0	baseline	recommended

4.1.4.1. Standard

All Oracle database control files should have consistent permission masks

4.1.4.2. Detailed Steps

- Do not alter the file ownership or the permissions of the database control file
- Ensure that the database control files are consistently protected

4.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.5. The owner of the database files should be Oracle

ID	Version	Level	Enforcement
ORAC-FP-2	1.0	baseline	recommended

4.1.5.1. Standard

The owner of the database files should be Oracle

4.1.5.2. Detailed Steps

- Set ownership of the database files to Oracle

4.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.6. Oracle users must not have greater access to the

database files than that set by the Oracle installation

ID	Version	Level	Enforcement
ORAC-FP-3	1.0	baseline	recommended

4.1.6.1. Standard

Oracle users must not have greater access to the database files than that set by the Oracle installation

4.1.6.2. Detailed Steps

- Do not grant greater than default file access to the Oracle database files to users

4.1.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.7. The database control file must be owned by Oracle

ID	Version	Level	Enforcement
ORAC-FP-4	1.0	baseline	mandatory

4.1.7.1. Standard

The database control file must be owned by Oracle

4.1.7.2. Detailed Steps

- Do not alter the file ownership or the permissions of the database control file

4.1.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.8. When assigning user rights to an object never use Grant All

ID	Version	Level	Enforcement
ORAC-FP-11	1.0	baseline	mandatory

4.1.8.1. Standard

When assigning user rights to an object never use Grant All

4.1.8.2. Detailed Steps

- Ensure that users are assigned only the specific rights they require

4.1.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may given to a user
- Unintended access may be given to a user
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.9. Database files should be protected from unauthorised access

ID	Version	Level	Enforcement
ORAC-FP-1	1.0	baseline	recommended

4.1.9.1. Standard

Database files should be protected from unauthorised access

4.1.9.2. Detailed Steps

- Set file access permissions on the database files to the least permissions required for satisfactory functioning.

4.1.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.10. The Oracle database initialisation file should be available to the Oracle system account alone

ID	Version	Level	Enforcement
ORAC-FP-7	1.0	baseline	recommended

4.1.10.1. Standard

The Oracle database initialisation file should be available to the Oracle system account alone

4.1.10.2. Detailed Steps

- Ensure that the file permissions on the database initialisation files do not permit user access

4.1.10.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The information held in the initialisation files can be used to subvert the database security
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.11. The Oracle database initialisation file must not be user readable

ID	Version	Level	Enforcement
ORAC-FP-6	1.0	baseline	mandatory

4.1.11.1. Standard

The Oracle database initialisation file must not be user readable

4.1.11.2. Detailed Steps

- Ensure that the file permissions on the database initialisation files do not permit user access

4.1.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The information held in the initialisation files can be used to subvert the database security
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.2. Administration

4.2.1. The use of quotas should be considered

ID	Version	Level	Enforcement
ORAC-ADMIN-2	1.0	baseline	recommended

4.2.1.1. Standard

The use of quotas should be considered to limit potentially harmful or unexpected growth in the database size

4.2.1.2. Detailed Steps

- Size the maximum extent of the projected database
- Implement a quota to limit the growth of the database to the maximum size expected

4.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and applications may be unavailable.

4.2.2. Maintain version control and change comments in the Oracle initialisation file

ID	Version	Level	Enforcement
ORAC-ADMIN-1	1.0	baseline	mandatory

4.2.2.1. Standard

Maintain version control and change comments in the Oracle initialisation file

4.2.2.2. Detailed Steps

- The file must include comments as to the change made
- The file must include initialisation values before and after the change
- The file must include who made the change and the date of the change

4.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised changes to the Oracle administration file may subvert the security of the database implementation.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.2.3. Check users privileges following an upgrade

ID	Version	Level	Enforcement
ORAC-ADMIN-3	1.0	baseline	mandatory

4.2.3.1. Standard

Following an Oracle upgrade, check that users privileges have not changed due to changes to role privileges.

4.2.3.2. Detailed Steps

- Note the users privilege levels
- Verify that post upgrade, users effective privilege levels have not increased

4.2.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Unintended privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.2.4. If using Oracle Enterprise Manager ensure the workstations/consoles on which it is run are protected from attack.

ID	Version	Level	Enforcement
ORAC-ADMIN-4	1.0	baseline	mandatory

4.2.4.1. Standard

If using Oracle Enterprise Manager ensure the workstations/consoles on which it is run are protected from attack.

4.2.4.2. Detailed Steps

- Implement password protected screensavers
- Implement an idle timeout facility to lock workstations

4.2.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.3. Backups

4.3.1. Online image backups should be taken

ID	Version	Level	Enforcement
ORAC-BACKUP-1	1.0	baseline	recommended

4.3.1.1. Standard

In accordance with the required backup schedule take periodic online image backups.

4.3.1.2. Detailed Steps

- Schedule periodic online image backups

4.3.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and applications may be unavailable.

4.3.2. Online incremental backups should be taken

ID	Version	Level	Enforcement
ORAC-BACKUP-2	1.0	baseline	recommended

4.3.2.1. Standard

In accordance with the required backup schedule take periodic online incremental backups.

4.3.2.2. Detailed Steps

- Schedule periodic online incremental backups

4.3.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and applications may be unavailable.

Chapter 5. Auditing and Monitoring

5.1. Events to be alerted in real-time

5.1.1. The system resource profile settings for password lock time should be set to forever

ID	Version	Level	Enforcement
ORAC-AUDI-1	1.0	baseline	recommended

5.1.1.1. Standard

The system resource profile settings for password lock time should be set to forever

5.1.1.2. Detailed Steps

- Define in the system resource profile settings password lock time to be forever.

5.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Setting password lock time to anything other than forever allows password guessing attempts to be resumed against the account after the lockout period expires
- Given enough time and enough attempts account passwords will be guessed
- Accounts may be compromised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.1.2. User accounts should be locked out after 3 consecutive login failures

ID	Version	Level	Enforcement
ORAC-AUDIT-1	1.0	baseline	recommended

5.1.2.1. Standard

User accounts should be locked out after 3 consecutive login failures

5.1.2.2. Detailed Steps

- Define the system resource profile settings to lock out accounts after 3 failures

5.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Given enough attempts any account password may be guessed
- Unauthorised access may result from allowing a liberal number of logon attempts
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2. Events to be audited

5.2.1. Enable auditing

ID	Version	Level	Enforcement
ORAC-AUDIT-3	1.0	baseline	recommended

5.2.1.1. Standard

Auditing should be enabled for the following events; - Create Table - Create Index - Drop Index - Alter Index - Drop Table - Audit Object - Noaudit Object - Create Database - Alter Database - Create Tablespace - Alter Tablespace - Drop Tablespace - Alter Session - Alter User - Alter System - Create User - Create Role - Drop User - Drop Role - Set Role - Create Schema - Create Control File - Create Trigger - Alter Trigger - Drop Trigger - Create Profile - Drop Profile - Alter Profile - Drop Procedure - Alter Role - Logon - Logoff - Logoff by Cleanup - System Audit - System Noaudit - Audit default - Noaudit default - System Grant - System Revoke - Grant Role - Revoke Role - Enable Trigger - Disable Trigger - Enable all Triggers - Disable all Triggers

5.2.1.2. Detailed Steps

- Enable auditing for the following events;
- - Create Table
- - Create Index

- - Drop Index
- - Alter Index
- - Drop Table
- - Audit Object
- - Noaudit Object
- - Create Database
- - Alter Database
- - Create Tablespace
- - Alter Tablespace
- - Drop Tablespace
- - Alter Session
- - Alter User
- - Alter System
- - Create User
- - Create Role
- - Drop User
- - Drop Role
- - Set Role
- - Create Schema
- - Create Control File
- - Create Trigger
- - Alter Trigger
- - Drop Trigger
- - Create Profile
- - Drop Profile
- - Alter Profile
- - Drop Procedure
- - Alter Role
- - Logon
- - Logoff

- - Logoff by Cleanup
- - System Audit
- - System Noaudit
- - Audit default
- - Noaudit default
- - System Grant
- - System Revoke
- - Grant Role
- - Revoke Role
- - Enable Trigger
- - Disable Trigger
- - Enable all Triggers
- - Disable all Triggers

5.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of accountability
- Legal or regulatory non-compliance
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2.2. The init.ora file must be modified for data dictionary auditing to be enabled.

ID	Version	Level	Enforcement
ORAC-AUDIT-6	1.0	baseline	recommended

5.2.2.1. Standard

The init.ora file must be modified for data dictionary auditing to be enabled.

5.2.2.2. Detailed Steps

- Edit the init.ora file and include the commands to enable data dictionary auditing

5.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of accountability
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2.3. Use triggers to capture audit information where it is not captured in table information

ID	Version	Level	Enforcement
ORAC-AUDIT-4	1.0	baseline	recommended

5.2.3.1. Standard

Use triggers to capture audit information where it is not captured in table information

5.2.3.2. Detailed Steps

- Before an insert, update or delete is executed use a trigger to write the audit information to a table.

5.2.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of accountability
- Legal or regulatory non-compliance
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2.4. Use triggers to log modifications to the DBA_USERS table

ID	Version	Level	Enforcement
ORAC-AUDIT-5	1.0	baseline	recommended

5.2.4.1. Standard

A trigger should be written to log modifications to the DBA_USERS table to identify user password substitution can be logged.

5.2.4.2. Detailed Steps

- Write a trigger that logs modifications to the DBA_USERS table.

5.2.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of accountability
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2.5. Tables should be designed to include extra fields for auditing actions taken

ID	Version	Level	Enforcement
ORAC-AUDIT-2	1.0	baseline	recommended

5.2.5.1. Standard

Tables should be designed to include extra fields for auditing actions taken

5.2.5.2. Detailed Steps

- When designing the tables include columns to capture information relating to changes to the data held in the row.

5.2.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of accountability
- Legal or regulatory non-compliance
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 6. Other

6.1. When an object is deleted from the database, delete all related synonyms

ID	Version	Level	Enforcement
ORAC-OTHER-1	1.0	baseline	mandatory

6.1.1. Standard

When an object is deleted from the database, delete all related synonyms

6.1.2. Detailed Steps

- When an object is to be deleted from the database ensure that all synonyms are identified and also deleted.

6.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 7. Checklist

<i>User Configuration</i>		
<i>User Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-UA-1	Are user profile names on the database consistent with their other login names?	
ORAC-UA-4	Are accounts belonging to personnel who have fixed periods of employments set up with account expiration dates?	
ORAC-AD-MIN-10	Do scripted modifications to users, use up to date commands?	
ORAC-UA-2	Do database administrators perform periodic user account audits to ensure access granted is still required?	
<i>Default Accounts</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-DA-5	Has the default password for the demo account been changed?	
ORAC-DA-3	Has the default password for the dbsnmp account been changed?	
ORAC-DA-4	Has the default password for the scott account been changed?	
ORAC-DA-6	Has the default password for the p08 account been changed?	
ORAC-DA-2	Has the default password for the system account been changed?	
ORAC-DA-1	Has the default password for the sys account been changed?	
ORAC-DA-7	Has the scott account been deleted?	
<i>Roles, Views, and Access Control</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-ACC-8	Are users with a requirement for a single role denied the ability to execute the set role command?	
ORAC-ACC-7	Is access to the operating system command line interface denied from users where possible?	
ORAC-ACC-4	Are password protected roles implemented?	
ORAC-ACC-1	Are views used to enforce access restrictions to tables?	
ORAC-ACC-3	Are users assigned any default Oracle roles?	
ORAC-ACC-6	For live database apps are the connect or resource roles used?	
ORAC-ACC-5	Are applications developed with password protected roles, without hard-coding the role password or disclosing the role password to the users?	
ORAC-ACC-2	Have database views been defined that map to database roles?	

Checklist

<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-PRIV-6	Has the CREATE privilege been granted to any application?	
ORAC-PRIV-5	Has the DROP privilege been granted to any application?	
ORAC-PRIV-4	Has the DBA role been granted to Database Administrators alone?	
ORAC-PRIV-11	Has the UNLIMITED TABLESPACE privilege been granted to any application?	
ORAC-PRIV-10	Has the EXECUTE ANY PROCEDURE privilege been granted to any application?	
ORAC-PRIV-1	If the scott account exists, does it have the CONNECT privilege only?	
ORAC-PRIV-12	Have all privileges been assigned to roles and not directly to users?	
ORAC-PRIV-7	Has the ALTER privilege been granted to any application?	
ORAC-PRIV-8	Has the BECOME USER privilege been granted to any application?	
ORAC-PRIV-9	Has the GRANT ANY PRIVILEGE/ROLE privilege been granted to any application?	
ORAC-PRIV-2	Does the p08 account have the DBA role revoked?	
<i>Authentication/Password Configuration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-AUTH-8	Is the sessions per user value set to 1?	
ORAC-AUTH-7	Is the Password reuse max value set to 12 passwords?	
ORAC-AUTH-5	Is the password lifetime set to 30 days?	
ORAC-AUTH-3	Do account logins timeout and disconnect after 30 minutes of inactivity?	
ORAC-AUTH-4	Is the password grace time set to 0 days?	
ORAC-AUTH-6	Is the Password lock time set to the maximum possible value?	
ORAC-UA-3	Are user accounts set such that the user can change their password?	
ORAC-AUTH-2	Do accounts have a password minimum length of 6 characters?	
ORAC-AUTH-1	Do accounts have a password minimum length of 6 characters?	
<i>Network Security Configuration</i>		

Checklist

<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-NET-5	Is the listener.ora file only readable by the administrators?	
ORAC-NET-1	Is Advanced Networking Option used to provide encrypted data transfer?	
ORAC-NET-2	Has the advanced networking option been implemented so as to protect Oracle passwords in transmission across the network?	
ORAC-NET-3	Are network listeners for SQL*NET clients password protected?	
ORAC-NET-4	Have the default passwords of the SQL*NET listeners been changed from the default value?	
<i>Configuration</i>		
<i>Files and File Permissions</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-FP-8	Is the config.ora file afforded the same control as the init.ora object?	
ORAC-FP-10	Is the object CATALOG.BSQ protected against modification?	
ORAC-FP-9	Is the object SQL.BSQ protected against modification?	
ORAC-FP-5	Do all Oracle database control files have consistent permission masks?	
ORAC-FP-2	Is the owner of the database files set to be Oracle?	
ORAC-FP-3	Do Oracle users have greater access to the database files than that set at installation time?	
ORAC-FP-4	Is the database control file owned by Oracle?	
ORAC-FP-11	Is Grant All used when assigning object access rights to a user?	
ORAC-FP-1	Are database files protected from unauthorised access?	
ORAC-FP-7	Is the Oracle database initialisation file available only to the Oracle system account?	
ORAC-FP-6	Are the Oracle database initialisation files user readable?	
<i>Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC-ADMIN-2	Are quotas used?	
ORAC-ADMIN-1	Are changes to the Oracle initialisation file commented and logged?	
ORAC-ADMIN-3	Are users privileges checked following an upgrade?	
ORAC-ADMIN-4	If using Oracle Enterprise Manager ensure the workstations/consoles on which it is run are protected from attack.	
<i>Backups</i>		

Checklist

<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC- BACKUP-1	Are online image backups taken periodically?	
ORAC- BACKUP-2	Are online incremental backups taken periodically?	
<i>Auditing and Monitoring</i>		
<i>Events to be alerted in real-time</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC- AUDI-1	Is the system resource profile settings for password lock time set to forever?	
ORAC- AUDIT-1	Are user accounts locked out after 3 consecutive login failures?	
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC- AUDIT-3	Is auditing enabled for the list of recommended events?	
ORAC- AUDIT-6	Has the init.ora file been modified to enable data dictionary auditing?	
ORAC- AUDIT-4	Are triggers used to capture audit information where it is not captured in table information?	
ORAC- AUDIT-5	Has a trigger been written to log modifications to the DBA_USERS table to identify user password substitution?	
ORAC- AUDIT-2	Are the tables designed to include extra fields for auditing actions taken?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
ORAC- OTHER-1	Is it ensured that when an object is deleted from the database, all related synonyms are also deleted?	