IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard – Oracle Database Security (SS-030)

Chief Security Office

Date: 04/07/ 2017

Department
for Work &
Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

Contents

1. Introduction

1.1. This Oracle Database Security Standard provides the list of controls that are required to secure Oracle implementations to a Department for Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data to be stored in Oracle Databases. It is to minimise the risk from known threats, both physical and logical, to an acceptable level for operations.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for Oracle Databases and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for Oracle deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits and IT Health Checks (ITHCs).

3. Exceptions

3.1. In this document the term “MUST” in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.4. Exceptions to this standard MUST be maintained on the application’s risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for consumption by suppliers, technical architects, database administrators, developers, security groups, and also IT staff such as security compliance teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier (including OFFICIAL-SENSITIVE) of the Government Security Classification Policy (GSCP). All of the organisation's Oracle implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all Oracle systems that are provisioned for departmental use.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

10.1. Oracle Database Installation and Patching Requirements

Reference	Security Control Requirement
10.1.1	**Ensure the appropriate version/patches for Oracle software is installed**. Using the most recent Oracle database software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software.
10.2.1	**Ensure all default passwords are changed.** Default passwords should be considered common knowledge to attackers, thus default passwords MUST be altered to mitigate unwanted authentication to the database.
10.3.1	**Ensure all sample data and users have been removed.** Sample data provides users with well-known default passwords, views, procedures and functions that could be used to exploit production environments.

10.2. Oracle Parameter Settings

10.2.1 Listener Settings

Reference	Security Control Requirement
10.2.1.1	**Ensure 'SECURE_CONTROL_<listener_name>' is set in 'listener.ora.** This setting determines the type of control connection the Oracle server requires for remote configuration of the listener. Listener configuration changes via unencrypted remote connections can result in unauthorised users sniffing the control configuration information from the network.
10.2.1.2	**Ensure 'extproc' is not present in 'listener.ora'**. `extproc` allows the database to run procedures from OS libraries, which in turn, can run any OS command. `extproc` should be removed to mitigate the risk that OS libraries can be invoked by the Oracle instance.
10.2.1.3	**Ensure 'ADMIN_RESTRICTIONS_<listener_name>' is set to 'ON'.** This setting means that any attempted real-time alteration of the parameters in the `listener` via the `set` command will be refused unless manually altered by a privileged user. By blocking unprivileged users from making alterations of the `listener.ora` file will help protect data confidentiality.
10.2.1.4	**Ensure 'SECURE_REGISTER_<listener_name>' is set to 'TCPS' or 'IPC'.** This setting specifies the protocols which are used to connect to the TNS listener.

10.2.2 Database Settings

Reference	Security Control Requirement
10.2.2.1	**Ensure ‘AUDIT_SYS_OPERATIONS’ is set to ‘TRUE’**. This setting provides for the auditing of all user activities conducted under the `SYSOPER` and `SYSDBA` accounts. If the parameter is set to `FALSE` then no statements except for `Startup/Shutdown` and `Logon` by `SYSDBA/SYSOPER` users will be audited.
10.2.2.2	**Ensure ‘AUDIT_TRAIL’ is set to ‘OS’, ‘DB,EXTENDED’, or ‘XML,EXTENDED’**. This setting determines whether or not Oracle’s basic audit features are enabled. Enabling 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.
10.2.2.3	**Ensure ‘GLOBAL_NAMES’ is set to ‘TRUE’.** This setting requires that the name of a database link matches that of the remote database it will connect to. If database connections weren’t allowed to match the domain that is being called remotely this could allow unauthorised domain sources to potentially connect via brute-force attacks.
10.2.2.4	**Ensure ‘LOCAL_LISTENER’ is set appropriately.** This setting specifies a network name that resolves to an address of the Oracle TNS listener. Unauthorised users with network access could redirect TNS network traffic to another system by registering a listener to the TNS listener, but by specifying the IPC protocol it is no longer possible to register listeners via TCP/IP.
10.2.2.5	**Ensure ‘07_DICTIONARY_ACCESSIBILITY’ is set to ‘FALSE’**. This setting is a database initialisations parameter that allows/disallows with the `EXECUTE ANY PROCEDURE` and `SELECT ANY DICTIONARY` access to objects in the `SYS` schema. Leaving the `SYS` schema open to connection could permit unauthorised access to critical data structures.
10.2.2.6	**Ensure ‘OS_ROLES’ is set to ‘FALSE’**. This setting permits externally created groups to be applied to database management. This could cause privilege overlaps and generally weaken security, thus should be set to `FALSE`.
10.2.2.7	**Ensure ‘REMOTE_LISTENER’ is empty.** This setting determines whether or not a valid listener can be established on a system separate from the database instance. As permitting a remote listener can allow for spoofing of connections which could compromise data confidentiality and integrity, this should be empty.
10.2.2.8	**Ensure ‘REMOTE_LOGIN_PASSWORDFILE’ is set to ‘NONE’**. This setting specifies whether or not Oracle checks for a password file during login and how many databases can be use the password file. The use of this sort of password login file could permit unsecured, privileged connections to the database, thus should be set to NONE.
10.2.2.9	**Ensure ‘REMOTE_OS_AUTHENT’ is set to ‘FALSE’**. This setting determines whether or not OS ‘roles’ with the attendant privileges are allowed for remote client connections. If set to `TRUE` this could allow the spoofing of connections and permit granting the privileges of an OS role to unauthorised users to make connections.
10.2.2.10	**Ensure ‘REMOTE_OS_ROLES’ is set to ‘FALSE’.** This setting permits remote users’ OS roles to be applied to database management. If `TRUE` this could cause privilege overlaps and generally weaken security.
10.2.2.11	**Ensure ‘UTIL_FILE_DIR’ is Empty**. The `utl_file_dir` setting allows packages to access and modify files specified `in utl_file_dir` and allows creation of directories and the manipulation of files in these directories. In addition, it has become a deprecated, legacy parameter, thus should be kept empty.
10.2.2.12	**Ensure ‘SEC_CASE_SENSITIVE_LOGON’ is set to ‘TRUE’**. This setting determines whether or not case-sensitivity is required for passwords during login. Due to the security bug CVE-2012-3137 it is recommended to set this parameter to `TRUE` if the October 2012 CPU/PSU or later was applied. If the patch was not applied it is recommended to set this parameter to `FALSE` to avoid that the vulnerability could be abused.

Reference	Security Control Requirement
10.2.2.13	**Ensure 'SEC_MAX_FAILED_LOGIN_ATTEMPTS' is set to '5'**. This parameter determines how many failed login attempts are allowed before Oracle closes the login connection. Allowing an unlimited number of login attempts for a user connection can facilitate both brute-force and Denial of Service (DoS) attacks.
10.2.2.14	**Ensure 'SEC_PROTOCOL_ERROR_FURTHER_ACTION' is set to 'DELAY,3' or 'DROP,3'**. This setting determines the Oracle server's response to bad/malformed packets received from the client. Malformed packets can potentially indicate packet-based attacks on the system, thus the value should be set accordingly.
10.2.2.15	**Ensure 'SEC_PROTOCOL_ERROR_TRACE_ACTION' is set to 'LOG'**. This setting determines the Oracle's server's logging response level to bad/malformed packets received from the client. Malformed packets can potentially indicate packet-based attacks on the system, thus the value should be set accordingly.
10.2.2.16	**Ensure 'SEC_RETURN_SERVER_RELEASE_BANNER' is set to 'FALSE'**. If set to `TRUE` this would allow the database to return information about the patch/update release number that is currently running on the database, this could facilitate unauthorised users to attempt to gain access based upon known patch weaknesses.
10.2.2.17	**Ensure 'SQL92_SECURITY' is set to 'FALSE'**. This setting prevents inadvertent information disclosure by ensuring that only users who already have `SELECT` privilege can execute the statements that would allow them to infer stored values.
10.2.2.18	**Ensure '_TRACE_FILES_PUBLIC' is set to 'FALSE'**. This setting determines whether or not the system's trace file is world readable. This should be restricted as permitting the read permission to other, anyone can read the instance's trace files file which could contain sensitive information about instance operations.
10.2.2.19	**Ensure 'RESOURCE_LIMIT' is set to 'TRUE'**. This setting determines whether resource limits are enforced in database profiles. If set to `TRUE`, this means the limits set in database profiles are enforced.

10.2.3 Files and File Permissions

Reference	Security Control Requirement
10.2.3.1	**The config.ora file MUST be afforded the same control as the init.ora object**. If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.2	**The object CATALOG.BSQ MUST not be modified.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.3	**The object SQL.BSQ MUST not be modified.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.4	**All Oracle database control files MUST have consistent permission masks**. If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.5	**Oracle users MUST not have greater access to the database files than that set by the Oracle installation**. If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.6	**Database files MUST be protected from unauthorised access**. Set file access permissions on the database files to the least permissions required for satisfactory functioning. If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.3.7	**The Oracle database initialisation file MUST be available to the Oracle system account alone.** If this is not applied the information held in the initialisation files can be used to subvert the database security.
10.2.3.8	**The Oracle database initialisation file MUST not be user readable**. If this is not applied the information held in the initialisation files can be used to subvert the database security.

10.2.4 Administration

Reference	Security Control Requirement
10.2.4.1	**The use of quotas MUST be considered to limit potentially harmful or unexpected growth in the database size**. If this is not applied, business information and applications may become unavailable.
10.2.4.2	**There MUST be maintenance of version control and change comments in the Oracle initialisation file**. The file must include comments as to the change made, the initialisation values before and after the change, who made the change and the date of the change. If this is not applied, this could lead to unauthorised changes to the Oracle administration file which may subvert the security of the database implementation.
10.2.4.3	**Following an Oracle upgrade, it MUST be checked that user's privileges have not changed due to changes to role privileges.** If this is not applied, unauthorised or unintended privileged access may be obtained.

10.2.5 Backups

Reference	Security Control Requirement
10.2.5.1	**Periodic online image backups MUST be taken In accordance with the required backup schedule**. If this is not applied, business information and applications may become unavailable.
10.2.5.2	**Periodic online incremental backups MUST be taken In accordance with the required backup schedule**. If this is not applied, business information and applications may become unavailable.

10.2.6 Network Interface Considerations

Reference	Security Control Requirement
10.2.6.1	**The listener.ora file MUST be readable only by the administrators.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.2.6.2	**The Advanced Networking Option MUST be used to provide encrypted data transfer**. Data transmitted in clear text is subject to modification and disclosure.
10.2.6.3	**Network listeners for SQL*NET clients MUST be password protected.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.

10.3. Oracle User Configurations

10.3.1 User Administration

Reference	Security Control Requirement
10.3.1.1	**User profile names on the database MUST be consistent with their other login names**. 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.
10.3.1.2	**Accounts belonging to personnel who have a fixed period of employment MUST be set up with expiration dates** Redundant accounts are often targeted to gain unauthorised access.
10.3.1.3	**Scripted modifications to users MUST use up to date commands.** Ensure that `alter user` is used instead of older commands, otherwise this could lead to compromise of data integrity and confidentiality.
10.3.1.4	**Database administrators MUST perform periodic user account audits to ensure access granted is still required.** Redundant accounts are often targeted to gain unauthorised access and redundant access rights can be used to perform unauthorised actions.

10.3.2 Roles, Views and Access Control

Reference	Security Control Requirement
10.3.2.1	**Users with a requirement for a single role MUST be denied the ability to execute the set role command.** Such users MUST not have access to the DBMS command prompt. Access to the CLI can be used to subvert the application security controls and the database security controls.
10.3.2.2	**Access to the operating system command line interface MUST be denied from users where possible.** Use the `product_profile` table to block the host command. Access to the CLI can be used to subvert the application security controls and the database security controls.
10.3.2.3	**Password protected roles MUST be implemented.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.3.2.4	**Views MUST be used to enforce access restrictions to tables.** Views can be defined by the data access requirements each role needs to have for the database. Otherwise inconsistent access control allows application restrictions to be bypassed.
10.3.2.5	**Users MUST not be assigned any default Oracle roles**. Users should be assigned appropriate created roles. Default roles may provide unintended access to the database.
10.3.2.6	**For live database, apps MUST not use the connect or resource roles.** `connect` or `resource` roles should not be assigned to users. This could lead to data being accidentally or maliciously altered or disclosed.
10.3.2.7	**Applications MUST be developed with password protected roles without hard-coding the role password or disclosing the role password to the users.** If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.
10.3.2.8	**Database views MUST be defined that map to database roles**. If this is not applied, this could lead to unauthorised users access to data that could be accidentally or maliciously altered or disclosed.

10.3.3 Oracle Connection and Login Restrictions

Reference	Security Control Requirement
10.3.3.1	**Ensure ‘FAILED_LOGIN_ATTEMPTS’ is less than or equal to ‘5’**. This setting determines how many failed login attempts are permitted before the system locks the user’s account. 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 Department.
10.3.3.2	**Ensure ‘PASSWORD_LOCK_TIME’ is greater than or equal to ‘1’**. This setting determines how many days must pass for the user’s account to be unlocked after the set number of failed login attempts have occurred. This value should be set according to the needs of the Department.
10.3.3.3	**Ensure ‘PASSWORD_LIFE_TIME’ is less than or equal to ‘90’**. This setting determines how long a password may be used before the user is required to change it. Allowing passwords to remain unchanged for long periods makes the success of brute-force attacks more likely. This value should be set according to the needs of the Department.
10.3.3.4	**Ensure ‘PASSWORD_REUSE_MAX’ is greater than or equal to ‘20’**. This setting determines how many different passwords must be used before the user is allowed to reuse a prior password. Allowing the reuse of a password within a short period of time after the password’s initial use can make the success of social-engineering and brute-force attacks more likely. This value should be set according to the needs of the Department.
10.3.3.5	**Ensure ‘PASSWORD_REUSE_TIME’ is greater than or equal to ‘365’**. This setting determines the amount of time in days that must pass before the same password may be reused. Reusing the same password after a short period of time has passed makes

Reference	Security Control Requirement
	the success of brute-force attacks more likely. This value should be set according to the needs of the Department.
10.3.3.6	**Ensure 'PASSWORD_GRACE_TIME' is less than or equal to '5'.** This setting determines how many days can pass after the user's password expires before the user's login capability is automatically locked out. This can help prevent password-based attacks against forgotten or disused accounts, while still allowing the account and its information to be accessible by DBA intervention.
10.3.3.7	**Ensure 'DBA_USERS.PASSWORD' is not set to 'EXTERNAL' for any user**. This setting determines whether or not a user can be authenticated by a remote OS to allow access to the database with full authorisation. Allowing remote OS authentication can potentially allow supposed privileged users to connect as authenticated, even when the remote system is compromised, thus these logins should be restricted.
10.3.3.8	**Ensure 'PASSWORD_VERIFY_FUNCTION' is set for all profiles**. This setting determines password settings requirements when a user password is changed at the SQL command prompt. This setting does not apply to users managed by the Oracle password file. Requiring users to apply such security features in password creation can potentially thwart logins by unauthorised users.
10.3.3.9	**Ensure 'SESSIONS_PER_USER' is less than or equal to '10'**. This setting determines the maximum number of user sessions that are allowed to be open concurrently. Limiting the number of user sessions can help prevent memory resource exhaustion by poorly formed requests or DoS attacks.
10.3.3.10	**Ensure no users are assigned the 'DEFAULT' profile**. Upon database creation users are assigned to the `DEFAULT` profile unless otherwise specified. Users should be created with role-based profiles. The `DEFAULT` profile has unlimited settings that are often required by the `SYS` user when patching; such settings should be tightly reserved.

10.3.4 Default Public Privileges for Packages and Object Types

Reference	Security Control Requirement
10.3.4.1	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_ADVISOR'**. The `DBMS_ADVISOR` package can be used to write files located on the server where the Oracle instance is installed. The use of this package could allow unauthorised users to corrupt OS files on the instance's host, so should be restricted.
10.3.4.2	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_CRYPTO'**. 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. An execution by the user `PUBLIC` can potentially endanger portions of or all of the data storage, so should be restricted.
10.3.4.3	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA'**. The `DBMS_JAVA` package can run Java classes or grant Java privileges. This could allow an attacker to run OS commands from the database, so should be restricted.
10.3.4.4	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA_TEST'**. The `DBMS_JAVA_TEST` package can run Java classes or grant Java privileges. This could allow an attacker to run OS commands from the database, so should be restricted.
10.3.4.5	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JOB'**. The `DBMS_JOB` package schedules and manages the jobs sent to the job queue. An unauthorised user could disable or overload the job queue, so should be restricted.
10.3.4.6	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LDAP'**. The `DBMS_LDAP` package contains functions and procedures that enable programmers to access data from LDAP servers. This package can be used to create specially crafted error messages or send information via DNA to the outside, so should be restricted.
10.3.4.7	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LOB'**. The `DBMS_LOB` package provides subprograms that can manipulate and read/write on BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs. An unauthorised user could

Reference	Security Control Requirement
	destroy data or cause a DoS condition due to corruption of disk space, so should be restricted.
10.3.4.8	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_OBFUSCATION_TOOLKIT'**. The `DBMS_OBFUSCATION_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. Allowing PUBLIC user privileges to access this capability can potentially harm the data storage, so should be restricted.
10.3.4.9	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_BACKUP_RESTORE'**. The `DBMS_RANDOM` package is used for generating random numbers but should not be used for cryptographic purposes. Use of this package can allow unauthorised application of the random number-generating function, so should be restricted.
10.3.4.10	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SCHEDULER'**. The `DBMS_SCHEDULER` package schedules and manages the database and OS jobs. Use of the package could allow an unauthorised user to run database or OS jobs, so should be restricted.
10.3.4.11	**Ensure 'EXECUTE' is revoked form 'PUBLIC' on 'DBMS_SQL'**. The `DBMS_SQL` package is used for running dynamic SQL statements. Use of the package could allow privilege escalation if the input validation is not done properly, so should be restricted.
10.3.4.12	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLGEN'.** The `DBMS_XMLGEN` package takes an arbitrary SQL query as input, converts it to XML format, and returns the result as a CLOB. Users could use this package to search the entire database for critical information like credit card numbers, and other sensitive information, so should be restricted.
10.3.4.13	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLQUERY'**. The `DBMS_XMLQUERY` package takes an arbitrary SQL query, converts it to XML format, and returns the result. Users could use this package to search the entire database for critical information like credit card numbers, and other sensitive information, so should be restricted.
10.3.4.14	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_FILE'**. The `UTL_FILE` package can be used to read/write files located on the server where the Oracle instance is installed. Use of this package could allow a user to read files at the OS. These files could contain sensitive information (e.g. password in `.bash_history`), so should be restricted.
10.3.4.15	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_INADDR'**. The `UTL_INADDR` package can be used to create specially crafted error messages or send information via DNS to the outside. This package can be used in SQL injection attacks from the web, so should be restricted.
10.3.4.16	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_TCP'**. The `UTL_TCP` package can be used to read/write files to TCP sockets on the server where the Oracle instance is installed. Use of this package could allow an unauthorised user to corrupt the TCP stream used to carry the protocols that communicate with the instance's external communications, so should be restricted.
10.3.4.17	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_MAIL'**. The `UTL_MAIL` package can be used to send email from the server where the Oracle instance is installed. Use of this package could allow an unauthorised user to corrupt the SMTP function to accept or generate junk email that can result in a DoS condition due to network saturation, so should be restricted.
10.3.4.18	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_SMTP'.** `The UTL_SMTP` package can be used to send email from the server where the Oracle instance is installed. Use of this package could allow an unauthorised user to corrupt the SMTP function to accept or generate junk email that can result in a DoS condition due to network saturation, so should be restricted.
10.3.4.19	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_DBWS'**. The `UTL_DBWS` package can be used to read/write file to web-based applications on the server where the Oracle instance is installed. Use of this package could allow an

Reference	Security Control Requirement
	unauthorised user to corrupt the HTTP stream used to carry the protocols that communicate with the instance's web-based external communications, so should be restricted.
10.3.4.20	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_ORAMTS'**. The `UTL_ORAMTS` package can be used to perform HTTP-requests. This could be used to send sensitive information to external websites, so should be restricted.
10.3.4.21	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_HTTP'**. The `UTL_HTTP` package can be used to perform HTTP-requests. This could be used to send sensitive information to external websites, so should be restricted.
10.3.4.22	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'HTTPURITYPE'**. The `UTL_HTTPURITYPE` package can be used to perform HTTP-requests. This could be used to send sensitive information to external websites, so should be restricted.

10.3.5 Revoke Non-Default Privileges for Packages and Object Types

Reference	Security Control Requirement
10.3.5.1	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SYS_SQL'**. The `DBMS_SYS_SQL` package is shipped as undocumented. Use of this package could allow a user to run code as a different user without entering user credentials, so should be restricted.
10.3.5.2	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_BACKUP_RESTORE'**. The `DBMS_BACKUP_RESTORE` package is used for applying PL/SQL commands to the native RMAN sequence. Use of this package could allow users to access file permissions on the OS level, so should be restricted.
10.3.5.3	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_AQADM_SYSCALLS'**. The `DBMS_AQADM_SYSCALLS` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.4	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_REPACT_SQL_UTL'**. The `DBMS_REPACT_SQL_UTL` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.5	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'INITJVMAUX'**. The `INITJVMAUX` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.6	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_STREAMS_ADM_UTL'** The `DBMS_STREAMS_ADM_UTL` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.7	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_AQADM_SYS'**. The `DBMS_AQADM_SQL` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.8	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_STREAMS_RPC'**. The `DBMS_STREAMS_RPC` package is shipped as undocumented and could allow unauthorised users to run SQL commands as user `SYS`, so should be restricted.
10.3.5.9	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_PRVTAQIM'**. The `DBMS_PRVTAQIM` package is shipped as undocumented and could allow unauthorised users to escalate privileges because any SQL commands could be executed as user `SYS`, so should be restricted.
10.3.5.10	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'LTADM'**. The `LTADM` package is shipped as undocumented and allows privilege escalation if granted to unprivileged users. Use of this package could allow an unauthorised user to run any SQL command as user `SYS`, so should be restricted.
10.3.5.11	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'WWV_DBMS_SQL'**. The `WWV_DBMS_SQL` package is shipped as undocumented and allows Oracle Application Express to run dynamic SQL statements. Use of this package could

Reference	Security Control Requirement
	allow an unauthorised user to run SQL statements as Application Express (APEX) user, so should be restricted.
10.3.5.12	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'WWV_EXECUTE_IMMEDIATE'**. The `WWV_EXECUTE_IMMEDIATE` package is shipped as undocumented and allows Oracle Application Express to run dynamic SQL statements. Use of this package could allow an unauthorised user to run SQL statements as Application Express (APEX) user, so should be restricted.
10.3.5.13	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_IJOB'**. The `DBMS_IJOB` package is shipped as undocumented and allows to run database jobs in the context of another user. Use of this package could allow an attacker to change identities by using a different username to execute a database job, so should be restricted.
10.3.5.14	**Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_FILE_TRANSFER'**. The `DBMS_FILE_TRANSFER` package allows to transfer files from one database server to another. Use of this package could allow an unauthorised user to transfer files from one database server to another, so should be restricted.

10.3.6 Revoke Excessive System Privileges

Reference	Security Control Requirement
10.3.6.1	**Ensure 'SELECT ANY DICTIONARY' is revoked from unauthorised 'GRANTEE'.** This privilege allows the grantee to access `SYS` schema objects. Using this privilege can give access to the Oracle password hashes part of the `SYS` schema, so should be restricted.
10.3.6.2	**Ensure 'SELECT ANY TABLE' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to open any table, except of `SYS`, to view it. Using this privilege can allow the unauthorised viewing of sensitive data, so should be restricted.
10.3.6.3	**Ensure 'AUDIT SYSTEM' is revoked from unauthorised 'GRANTEE'**. This keyword allows the change of auditing activities on the system. Using this privilege can allow the unauthorised alteration of system audit activities and disabling the creation of audit trails, so should be restricted.
10.3.6.4	**Ensure 'EXEMPT ACCESS POLICY' is revoked from unauthorised 'GRANTEE'**. This privilege provides the grantee the capability to access all the table rows regardless of row-level security lockouts. Using this privilege can allow an unauthorised user to potentially access and change confidential data, so should be restricted.
10.3.6.5	**Ensure 'BECOME USER' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to inherit the rights of another user. Using this privilege can allow the unauthorised use of another user's privilege, so should be restricted.
10.3.6.6	**Ensure 'CREATE PROCEDURE' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to create a stored procedure that will fire when given the correct command sequence. Using this privilege can allow unauthorised users to cause severe problems, such as, rogue procedures facilitating data theft or DoS by corrupting data tables, so should be restricted.
10.3.6.7	**Ensure 'ALTER SYSTEM' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to dynamically alter the instance's running operations. Using this privilege can allow unauthorised users to cause severe problems, such as, instance sessions being killed or the stopping of redo log recording, which would make transactions unrecoverable, so should be restricted.
10.3.6.8	**Ensure 'CREATE ANY LIBRARY' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to create objects that are associated to the shared libraries. Using this privilege can allow the creation of numerous library-associated objects and potentially corrupt the libraries' integrity, so should be restricted.
10.3.6.9	**Ensure 'CREATE LIBRARY' is revoked from unauthorised 'GRANTEE'**. This privilege allows the grantee to create objects that are associated to the shared libraries. Using this privilege can allow the creation of numerous library-associated objects and potentially corrupt the libraries' integrity, so should be restricted.

Reference	Security Control Requirement
10.3.6.10	**Ensure 'GRANT ANY OBJECT PRIVILEGE' is revoked from unauthorised 'GRANTEE'**. This keyword provides the grantee the capability to grant access to any single or multiple combinations of objects to any grantee in the catalog of the database. Using this privilege can allow an unauthorised user to potentially access and change confidential data or damage the data catalog due to potential complete instance access, so should be restricted.
10.3.6.11	**Ensure 'GRANT ANY ROLE' is revoked from unauthorised 'GRANTEE'**. This keyword provides the grantee the capability to grant any single role to any grantee in the catalog of the database. Using this privilege can allow an unauthorised user to potentially access and change confidential data or damage the data catalog due to potential complete instance access, so should be restricted.
10.3.6.12	**Ensure 'GRANT ANY PRIVILEGE' is revoked from unauthorised 'GRANTEE'**. This keyword provides the grantee the capability to grant any single privilege to any item in the catalog of the database. Using this privilege can allow an unauthorised user to potentially access and change confidential data or damage the data catalog due to potential complete instance access, so should be restricted.

10.3.7 Revoke Role Privileges

Reference	Security Control Requirement
10.3.7.1	**Ensure 'DELETE_CATALOG_ROLE' is revoked from unauthorised 'GRANTEE'**. This setting provides `delete` privileges for the records in the systems audit table. Unauthorised access to this privilege can allow the destruction of audit records vital to the forensic investigation of unauthorised activities, so should be restricted.
10.3.7.2	**Ensure 'SELECT_CATALOG_ROLE' is revoked from unauthorised 'GRANTEE'**. This setting provides `select` privileges on all data dictionary views held in the `SYS` schema. Unauthorised access to this privilege can allow the disclosure of all dictionary data, so should be restricted.
10.3.7.3	**Ensure 'EXECUTE_CATALOG_ROLE' is revoked from unauthorised 'GRANTEE'**. This setting provides `executive` privileges for a number of packages and procedures in the data dictionary in the `SYS` schema. Unauthorised access to this privilege can allow the disruption of operations by initialisation of rogue procedures, so should be restricted.
10.3.7.4	**Ensure 'DBA' is revoked from unauthorised 'GRANTEE'**. The DBA role is the default database administrator role provided for the allocation of administrative privileges. Unauthorised assignment of the DBA role can lead to data breaches, integrity violations and DoS conditions, so should be restricted.

10.3.8 Revoke Excessive Table and View Privileges

Reference	Security Control Requirement
10.3.8.1	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'AUD$'**. The `SYS.AUD$` table contains all the audit records for the database of the non-DML events. Permitting non-privileged users the authorisation to manipulate the `SYS.AUD$` table can allow distortion of the audit records and hiding unauthorised activities, so should be restricted.
10.3.8.2	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'USER_HISTORY$'**. The `SYS.USER_HISTORY$` table contains all the audit records for the user's password change history. Permitting non-privileged users the authorisation to manipulate records in the `SYS.USER_HISTORY$` table can allow distortion of the audit trail and potentially hiding unauthorised data confidentiality attacks or integrity changes, so should be restricted.
10.3.8.3	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'LINK$'**. The `SYS.LINK$` table contains all the user's password information and data table link

Reference	Security Control Requirement
	information. Permitting non-privileged users to manipulate the `SYS.LINK$` table can allow capture of password information and/or corrupt the primary database linkages, so should be restricted.
10.3.8.4	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'SYS.USER$'**. The `SYS.USER$` table contains the user's hashed password information. Permitting non-privileged users the authorisation to open the `SYS.USER$` table can allow the capture of password hashes for the later application of password cracking algorithms to breach confidentiality, so should be restricted.
10.3.8.5	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'DBA_%'**. The `DBA_` views show all the information which is relevant to administrative accounts. Permitting users the authorisation to manipulate the `DBA_` views can expose sensitive data, so should be restricted.
10.3.8.6	**Ensure 'ALL' is revoked from unauthorised 'GRANTEE' on 'SYS.SCHEDULER$_CREDENTIAL'**. The `SCHEDULER$_CREDENTIAL` table contains the database scheduler credential information. Permitting non-privileged users the authorisation to open the `SCHEDULER$_CREDENTIAL` table, so should be restricted.
10.3.8.7	**Ensure 'SYS.USER$MIG' has been dropped**. The `SYS.USER$MIG` table is created during migration and contains the Oracle password hashes before the migration starts. This table is not deleted after the migration, thus an attacker could access the table containing the Oracle password hashes, so should be restricted.

10.3.9 Miscellaneous Access and Authorisation restrictions

Reference	Security Control Requirement
10.3.9.1	**Ensure '%ANY%' is revoked from unauthorised 'GRANTEE'**. This keyword provides the user the capability to alter any item in the catalog of the database. Using the `ANY` expansion of a privilege can allow an unauthorised user to potentially change confidential data or damage the data catalog, so should be restricted.
10.3.9.2	**Ensure 'DBA_SYS_PRIVS.%' is revoked from unauthorised 'GRANTEE' with 'ADMIN_OPTION' set to 'YES'**. This privilege allows the designated user to grant another user the same privileges. Using this privilege can allow the granting of a restricted privilege to an unauthorised user, so should be restricted.
10.3.9.3	**Ensure proxy users have only 'CONNECT' privilege**. A proxy user should only have the ability to connect to the database and should not have privileges granted directly to them.
10.3.9.4	**Ensure 'EXECUTE ANY PROCEDURE' is revoked from 'OUTLN'**. Migrated `OUTLN` users have more privileges than required, remove any unneeded privileges.
10.3.9.5	**Ensure 'EXECUTE ANY PROCEDURE' is revoked from 'DBSNMP'**. Migrated `DBSNMP` users have more privileges than required, remove any unneeded privileges.

10.4. Audit/Logging Policies and Procedures

Reference	Security Control Requirement
10.4.1	**Auditing MUST be enabled for the following events:** **Enable ‘USER’ audit option** **Enable ‘ALTER USER’ audit option** **Enable ‘DROP USER’ audit option** **Enable ‘ROLE’ audit option** **Enable ‘SYSTEM GRANT’ audit option** **Enable ‘PROFILE’ audit option** **Enable ‘ALTER PROFILE’ audit option** **Enable ‘DROP PROFILE’ audit option** **Enable ‘DATABASE LINK’ audit option** **Enable ‘PUBLIC DATABASE LINK’ audit option** **Enable ‘PUBLIC SYNONYM’ audit option** **Enable ‘SYNONYM’ audit option** **Enable ‘GRANT DIRECTORY’ audit option** **Enable ‘SELECT ANY DICTIONARY’ audit option** **Enable ‘GRANT ANY OBJECT PRIVILEGE’ audit option** **Enable ‘GRANT ANY PRIVILEGE’ audit option** **Enable ‘DROP ANY PROCEDURE’ audit option** **Enable ‘ALL’ audit option on ‘SYS.AUD$’** **Enable ‘PROCEDURE’ audit option** **Enable ‘ALTER SYSTEM’ audit option** **Enable ‘TRIGGER’ audit option** **Enable ‘CREATE SESSION’ audit option** Where these are not applied could result in loss of accountability and legal or regulatory non-compliance.
10.4.2	**The init.ora file MUST be modified for data dictionary auditing to be enabled.** Where these are not applied could result in loss of accountability.
10.4.3	**Triggers MUST be used to capture audit information where it is not captured in table information**. Before an insert, update or delete is executed use a trigger to write the audit information to a table. Where these are not applied could result in loss of accountability and legal or regulatory non-compliance. Fine Grained Auditing can capture additional information such as application context, location etc.
10.4.4	**A trigger MUST be written to log modifications to the DBA_USERs table to identify user password substitution can be logged.** Where these are not applied could result in loss of accountability.
10.4.5	**Tables MUST be designed to include extra fields for auditing actions taken**. When designing the tables include columns to capture information relating to changes to the data held in the row. Where these are not applied could result in loss of accountability and legal or regulatory non-compliance. These should be hidden columns and thus not viewable by non-privileged users.

10.5. Recommended Oracle Add-on products

10.5.1 Oracle Database Security Assessment Tool

In addition to implementing the control requirements outlined above it is recommended that projects utilising this document make use of the Oracle Database Security Assessment Tool (DBSAT) before and after adopting the necessary control requirements. An overview of DBSAT is given here:

The Oracle Database Security Assessment Tool is a free resource that analyses database configurations and security policies to uncover security risks and improve the security posture of Oracle Databases within the Department. It can be used to implement and enforce security best practices.

DBSAT reports on the state of user accounts, role and privilege grants, and policies that control the use of various security features in the database. This information can be used to fix immediate short-term risks and implement a comprehensive security strategy.

The tool consists of two components, the DBSAT Collector and the DBSAT Reporter that correspond to the functions of data collection and data analysis respectively:

- The DBSAT Collector executes and runs operating system commands to collect data from the system to be assessed. It does this primarily by querying database dictionary views. The collected data is written to a file that is used by the DBSAT Reporter in the analysis phase.
- The DBSAT Reporter analyses the collected data and reports its findings and recommendations in multiple formats: PDF, Excel, and Text. The Reporter can run on any machine: PC, laptop, or server. You are not limited to running it on the same server as the Collector.

DBSAT can be used to:

- Quickly identify security configuration errors databases
- Promote security best practices
- Improve the security posture of Oracle Databases
- Reduce the attack surface and exposure to risk

Certain requirements must be met in order to install and use DBSAT successfully:

Reference	Security Control Requirement
10.5.1.1	**The DBSAT Reporter is a platform-independent Python program and requires Python 2.6 or later to run.**

10.5.1.2	**The Zip and Unzip utilities must be situated in the appropriate locations.** Both the DBSAT Collector and Reporter use Zip and Unzip utilities already installed on the system to encrypt the generated files. The DBSAT tool expects to find these utilities in the locations shown below. It the utilities are elsewhere they must be updated accordingly:
	Windows (dbsat.bat script):
	`SET ZIP_CMD=%ORACLE_HOME%\bin\zip.exe`
	`SET UNZIP_CMD=%ORACLE_HOME%\bin\unzip.exe`
	All other platforms (dbsat script)
	`ZIP=/usr/bin/zip`
	`UNZIP=/usr/bin/unzip`
	`DBZIP=${ORACLE_HOME}/bin/zip`

Reference	Security Control Requirement
10.5.1.3	**The DBSAT tool can only be run on Oracle Database 10.2.0.5 and later releases**
10.5.1.4	**The DBSAT Collector MUST be run on a server that contains the database.** In addition, the DBSAT Collector MUST be run as an OS user with read permissions on files and directories under `ORACLE_HOME` in order to collect and process file system data using OS commands.
10.5.1.5	**The DBSAT Collector MUST connect to the database as a user with sufficient privileges.** The DBSAT Collector collects most of its data by querying database views, thus it needs the necessary privileges to select from these views. The DBSAT user MUST be granted the following privileges: • `CREATE SESSION` • `SELECT` on `SYS.REGISTRY$HISTORY` • Role `SELECT_CATALOG_ROLE` • Role `DV_SECANALYST` (if Database Vault is enabled) • Role `AUDIT_VIEWER` (12c only) • Role `CAPTURE_ADMIN` (12c only) • `SELECT` on `SYS.DBA_USERS_WITH_DEFPWD` (11g and 12c) • `SELECT` on `AUDSYS.AUD$UNIFIED` (12c only)
10.5.1.6	**The output files from the DBSAT Collector and the DBSAT Reporter are sensitive as they may reveal weaknesses in the security posture of the database. To prevent unauthorised access to these files, the following security measures MUST be implemented:** • Ensure that the directories holding these files are secured with the appropriate permissions. • Delete the files securely after the recommendations they contain have been implemented. • Share them with others in their (by default) encrypted form. • Grant user permissions on a short-term basis and revoke these when no longer necessary.

10.5.2 Database Vault Security Guide

Oracle Database Vault protects data at the source from privilege abuse by identifying privileged users and then implementing least privilege and separation of duties principles at the data level. Database Vault should be mandatory for new Oracle production and pre-production databases and retro-fitted to any remediated production and pre-production instances.

Reference	Security Control Requirement
10.5.2.1	**“Separation of duties” MUST be utilised and enforced.** Meaning that you restrict each user’s privileges only to the tasks they are responsible for, and no more – separation of duties strengthens security by separating security-related administration from day-to-day DBA operations.
10.5.2.2	**There MUST be separate accounts for database account management, database security administration, and additional named accounts for backup operations.**
10.5.2.3	**There MUST be a matrix for separation of duties**. This can help plan the Database Vault deployment.
10.5.2.4	**The following tasks MUST be documented:**

Reference	Security Control Requirement
	• The responsibilities of each administrative user • The kind of access users need. For example, application owners should have data access and developers need access to development instances only. • Who must manage the system without accessing business data (for example, users who perform backup, patching, tuning, and monitoring operations). • The duties of each category of tasks (for example, the files that must be backed up, the applications that require patching, what exactly is monitored). Include the alternate user accounts for each of these tasks. • The databases and applications that must be protected. This includes Oracle applications, partner applications, and custom applications. • Who must be authorized to access business data, including the following: o Application owners through middle tier processes o Business users through an application interface • Emergency "what if" scenarios, such as how to handle a security breach • Reporting in a production environment, which should include the following: o Who runs the reports o Which reports must be run o The frequency with which each report is run o The users who must receive a copy of each report • In addition to a separation of duty matrix, the creation of the following matrices: o An Oracle Database Vault-specific matrix, which can cover the names and tasks of users who have been granted Database Vault roles o An application protection matrix, which can cover the applications to be protected and the types of protections you have put in place.
10.5.2.5	**The SYSTEM account should not be used for general database administration**. The SYSOPER or SYSDBA roles should be assigned to the relevant authorised users.
10.5.2.6	**There MUST be no application tables created in the SYSTEM schema unless done so by a COTS application.** Any application design MUST avoid creating tables in the SYS or SYSTEM schemas.
10.5.2.7	**Limit the SYSDBA privilege only to users who must connect using this privilege when absolutely necessary and for applications that still require SYSDBA access.** Such as Oracle Recovery Manager (RMAN) and mandatory patching processes. For all other cases, create named database accounts to perform daily database administration.
10.5.2.8	**When running Oracle Database Vault in a production environment, follow these guidelines:** • Run a full test of the applications to ensure that the Database Vault policies which have been created are working as expected. • Monitor the performance of the applications, and if necessary, tune the rule expressions. • Assign responsibilities to the appropriate production support and security groups, as follows: o Assign security responsibilities to the database security administrator. o Assign account management to the database account manager. o Assign resource management tasks to database administrators.

Reference	Security Control Requirement
	• Back up your Database Vault API scripts to a secure server.
10.5.2.9	**The recycle bin feature MUST be disabled to better secure realm-protected objects.** If the recycle bin is enabled, realm-protected objects that are dropped go into the recycle bin. Once there, the objects are no longer protected by the realm.
10.5.2.10	**Ensure 'CREATE EXTERNAL JOB' is revoked from users who do not need it.** The `CREATE EXTERNAL JOB` privilege is required for database users who want to execute jobs that run on the operating system outside the database. By default, this privilege is granted to all users who have been granted the `CREATE JOB` privilege. Thus, MUST be revoked from users who do not require it.

10.5.3 Oracle Advanced Security

Oracle Advanced Security offers two main features for protecting sensitive information in databases. The first, Oracle Transparent Data Encryption (TDE) is a flexible encryption solution that allows for either column encryption or complete tablespace encryption. The second, Oracle Data Redaction, removes or redacts columns of sensitive data in real time during output to applications.

10.5.3.1 Oracle Transparent Data Encryption

10.5.3.1.1	**The following MUST be considered:** • Identify the degrees of sensitivity of data in your database, the protection that they need, and the levels of risk to be addressed. For example, highly sensitive data requiring stronger protection can be encrypted with the AES256 algorithm. A database that is not as sensitive can be protected with no salt or the `nomac` option to enable performance benefits. • Evaluate the costs and benefits that are acceptable to data and keystore protection. Protection of keys determines the type of keystore to be used: auto-login software keystores, password-based software keystores, or hardware keystores. • Consider having separate security administrators for TDE and for the database. • Consider having a separate and exclusive keystore for TDE, such as Oracle Key Vault. • Implement protected back-up procedures for your encrypted data • Consider the use of tablespace encryption vs. column encryption • Consider the preferred cryptographic algorithms/strengths
10.5.3.1.2	**Old plaintext fragments may be present for some time until the database overwrites the blocks containing such values. If privileged operating system users bypass the access controls of the database, then they might be able to directly access these values in the data file holding the tablespace.** **To minimize this risk:** • Create a new tablespace in a new data file. You can use the `CREATE TABLESPACE` statement to create this tablespace. • Move the table containing encrypted columns to the new tablespace. You can use the `ALTER TABLE…..MOVE` statement. • Repeat this step for all of the objects in the original tablespace. • Drop the original tablespace. You can use the `DROP TABLESPACE` *`tablespace`* `INCLUDING CONTENTS KEEP DATAFILES` statement. Oracle recommends that you securely delete data files using platform-specific utilities. • Use platform-specific and file system-specific utilities to securely delete the old data file. Examples of such utilities include `shred` (on Linux) and `sdelete` (on Windows).

10.5.3.1.1	**The following MUST be considered:** • Identify the degrees of sensitivity of data in your database, the protection that they need, and the levels of risk to be addressed. For example, highly sensitive data requiring stronger protection can be encrypted with the AES256 algorithm. A database that is not as sensitive can be protected with no salt or the `nomac` option to enable performance benefits. • Evaluate the costs and benefits that are acceptable to data and keystore protection. Protection of keys determines the type of keystore to be used: auto-login software keystores, password-based software keystores, or hardware keystores. • Consider having separate security administrators for TDE and for the database. • Consider having a separate and exclusive keystore for TDE, such as Oracle Key Vault. • Implement protected back-up procedures for your encrypted data • Consider the use of tablespace encryption vs. column encryption • Consider the preferred cryptographic algorithms/strengths

10.5.3.2 Oracle Data Redaction

Reference	Security Control Requirement
10.5.3.2.1	**The following MUST be considered:** • Oracle Data Redaction is not intended to protect against attacks by privileged database users who run ad hoc queries directly against the database. • Oracle Data Redaction is not intended to protect against users who run exhaustive SQL queries that attempt to determine the actual values by **inference**. • Oracle Data Redaction relies on the database and application context values. For applications, it is the responsibility of the application to properly initialize the context value. • Oracle Data Redaction is not enforced for users who are logged in using the `SYSDBA` administrative privilege. • Certain DDL statements that attempt to copy the **actual data** out from under the control of a data redaction policy (that is, `CREATE TABLE AS SELECT`, `INSERT AS SELECT`) are blocked by default, but you can disable this behavior by granting the user the `EXEMPT REDACTION POLICY` system privilege • Oracle Data Redaction does not affect day-to-day database operations, such as backup and recovery, Oracle Data Pump exports and imports, Oracle Data Guard operations, and replication. • Do not include any redacted columns in a SQL expression that is used in a `GROUP BY` clause in a SQL statement. Oracle does not support this behavior, and raises an `ORA-00979: not a GROUP BY expression` error. This happens because internally the expression in the `SELECT` list must be modified by Data Redaction, but this causes it to no longer be found when it comes time to process the `GROUP BY` clause (which is currently not updated by Data Redaction) leading to this unintended error message.
10.5.3.2.2	**There MUST be restrictions on the list of users who can create, view and edit Data Redaction policies**. This can be applied by limiting who has the `EXECUTE` privilege on the `DBMS_REDACT` package and by limiting who has the `SELECT` privilege on the `REDACTION_POLICIES` and `REDACTION_COLUMNS` views.

Reference	Security Control Requirement
10.5.3.2.3	**There MUST be restrictions on who is exempted from redaction.** This can be applied by limiting the `EXEMPT REDACTION POLICY` privilege. If Oracle Database Vault is used to restrict privileged user access, then realms can be used to restrict granting of `EXEMPT REDACTION POLICY`.
10.5.3.2.4	Both users `SYS` and `SYSTEM` automatically have the `EXEMPT REDACTION POLICY` system privilege. (`SYSTEM` has the `EXP_FULL_DATABASE` role, which includes the `EXEMPT REDACTION POLICY` system privilege.) This means that the `SYS` and `SYSTEM` users can always bypass any existing Oracle Data Redaction policies, and will always be able to view data from tables (or views) that have Data Redaction policies defined on them. Be mindful of the following: • Do not create Data Redaction policies on the default Oracle Database schemas, including the `SYS` and `SYSTEM` schemas. • Be aware that granting the `EXEMPT DATA REDACTION` system privilege to additional roles may enable users to bypass Oracle Data Redaction, because the grantee role may have been granted to additional roles. • Do not revoke the `EXEMPT DATA REDACTION` system privilege from the roles that it was granted to by default.
10.5.3.2.5	When writing a policy expression that depends on a `SYS_CONTEXT` attribute that is populated by an application, the application might not always populate that attribute. If the user is able to connect directly (rather than through the application), then the `SYS_CONTEXT` attribute would not have been populated. This `NULL` scenario MUST be handled in your policy expression, otherwise you could unintentionally reveal actual data to the querying user.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	When the next ITHC is performed on the application in question.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

10. Security Standards Reference List

Document Name	Location	Version
Security Standards master list		

11. Reference Documents

CISecurity.org. (2016) *CIS Oracle 11g R2 Benchmark* v.2.2.0 [online] 31st May 2016. Available from:

https://benchmarks.cisecurity.org/tools2/oracle/CIS_Oracle_Database_11g_R2_Benchmark_v2.2.0.pdf. [Accessed: 30th September 2016]

O'Dwyer Frank. (2009) *Oracle Database Management System Security Standard* [online] 16th May 2009. Available from: http://www.frankodwyer.com/standards/index.html#db. [Accessed: 30th September 2016]

Oracle.com (2016) *Configuring Network Data Encryption and Integrity for Oracle Servers and Clients* [online] 11th February 2016. Available from: https://docs.oracle.com/cd/E11882_01/network.112/e40393/preface.htm#ASOAG10081. [Accessed: 2nd November 2016]

Red-database-security.com (2016) *Best Practice for Oracle Databases* [online]. Available from: http://www.red-database-security.com/wp/sentrigo_webinar.pdf. [Accessed: 3rd November 2016]

Security.uri.edu (2015) *CIS Oracle Database 12c Benchmark* [online] 29th April 2015. Available from: https://security.uri.edu/uploads/CIS_Oracle_Database_12c_Benchmark_v1.0.0.pdf. [Accessed: 20th November 2016]

12. Definition of Terms

Terms	Definition
Brute-force Attack	A brute-force attack is a password and cryptography attack that does not attempt to decrypt any information, but continue to try a list of different passwords, words, or letters.
Denial of Service	A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system.
Listener	The listener is a separate process that runs on the database server computer. It receives incoming client connection requests and manages the traffic of these requests to the database server.
Sniffing	Sniffing allows individuals to capture data as it is transmitted over a network and is used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.
Spoofing	A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.
SQL Injection	SQL Injection refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

13. Glossary

BFILE	Binary Files
BLOB	Binary Large Object
CLOB	Character Large Object
COTS	Commercial off-the-shelf
CPU	Critical Patch Updates
DA	Design Authority (DA)
DBA	Database Administrator
DML	Data Manipulation Language
DNA	Distributed Numeric Assignment
DNS	Domain Name System
DoS	Denial of Service
DWP	Department of Work and Pensions (DWP)
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPC	Inter Process Communications
LDAP	Lightweight Directory Access Protocol
LOB	Large Object
NCLOB	National Character Large Object
OS	Operating System
PL	Procedural Language
PSU	Patch Set Updates
RMAN	Recovery Manager
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TDE	Transparent Data Encryption
TNS	Transparent Network Substrate
XML	Extensible Markup Language

14. Controls Catalogue Mapping

The requirements in this document are derived from the high-level controls prescribed in the DWP Controls Catalogue