CXL SECURE

AZScan

Report for
Demo

07-Dec-2008 21:34

Report for	Demo
Company	CXL Finance
Business Unit	Finance Division
Location	London
System	

Report Name	c:\tbxnew-works\reports\myrepo.doc
Report Date	07-Dec-2008 21:34

Key to colors

Risks	L Low risk	M Medium risk	H High risk
Results	L Correct or low risk	M Medium impact	H Major problem

1 USERSCCUsers

1.1	STDACC	H Standard accounts	H 18
1.2	FAILLOG	L Failed logins allowed	H 32

2 PASSWORDSPasswords

2.1	PWDCHNG	L Password last changed	H 4
2.2	PWDGRACE	L Password grace time	H 32
2.3	PWDLIFE	H Password life time	H 34
2.4	PWDLOCK	L Password lock time	L 0
2.5	PWDREUSENO	M Password reuse number	H 62
2.6	PWDREUSETIME	M Password reuse time	H 34
2.7	PWDVERIFY	L Password verify function	H 34

3 PROFILESUser profiles

3.1	DEFPROF	L The DEFAULT profile	H 28
3.2	OTHPROF	L Other profiles	H 5

4 PRIVILEGESPrivileges

4.1	OSYSPRIV	M User's system privileges	L 0
4.2	OPQUANY	M Users with ANY privilege	H 657

5 ROLESRoles

5.1	OROLDBA	H Users granted the DBA Role	M 3
5.2	OROLANY	M Roles with ANY privilege	H 97
5.3	OROLPWD	L Roles without passwords	H 33
5.4	OROLPUB	M Roles granted to PUBLIC	L 0

6 SYSTEMSystem settings

6.1	SYSLOGPWDFILE	M Remote login password file	L 1
6.2	SYSOSAUTH	H Remote OS authentication	L 1

6.3	SYSDATADIC	(M) Data dictionary Accessibility	(L) 1

1 USERSCC - Users

RISKS

In this section we look at some of the user settings which effect the security of the system.

1.1 STDACC - Standard accounts

H

RISKS

When Oracle is installed, a number of standard accounts are also included. Many of these have default passwords which are now well known and many have a password which is the same as the user-ID.
Accounts with known passwords can be logged into unless they are locked. An 'L' beside an account indicates that it is locked.

ACTIONS

Examine each of these accounts and change the password.

H

RESULTS

Standard accounts with unchanged passwords.

User account	Password	
CTXSYS	CHANGE_ON_INSTALL	L
DIP	DIP	L
DMSYS	DMSYS	L
EXFSYS	EXFSYS	L
HR	CHANGE_ON_INSTALL	L
MDDATA	MDDATA	L
MDSYS	MDSYS	L
OE	CHANGE_ON_INSTALL	L
OLAPSYS	MANAGER	L
ORDPLUGINS	ORDPLUGINS	L
ORDSYS	ORDSYS	L
OUTLN	OUTLN	L
PM	CHANGE_ON_INSTALL	L
SCOTT	TIGER	
SH	CHANGE_ON_INSTALL	L
SI_INFORMTN_SCHEMA	SI_INFORMTN_SCHEM	L
WMSYS	WMSYS	L
XDB	CHANGE_ON_INSTALL	

18 standard accounts were found to have default passwords.

Accounts marked with 'L' are locked.

1.2 FAILLOG - Failed logins allowed

L

RISKS

The number of failed attempts to log in to the user account before the account is locked. This protects the system from people trying to guess passwords.
Setting this to 'Unlimited' means that the account is not locked by failed passwords.

ACTIONS

Set this parameter to a low number between 3 and 6 using profiles.

H

RESULTS

Failed Login attempts settings.

User	Setting	Profile	
ANONYMOUS	10	DEFAULT	L
BI	10	DEFAULT	L
CTXSYS	10	DEFAULT	L
CXL_USER1	10	DEFAULT	
CXL_USER2	16	PROFILE3	
CXL_USER3	UNLIMITED	MONITORING_PROFILE	L
CXLUSER11	10	DEFAULT	
DAVE1	10	DEFAULT	
DBSNMP	UNLIMITED	MONITORING_PROFILE	
DIP	10	DEFAULT	L
DMSYS	10	DEFAULT	L
EXFSYS	10	DEFAULT	L
HR	10	DEFAULT	L
IX	10	DEFAULT	L
MDDATA	10	DEFAULT	L
MDSYS	10	DEFAULT	L
MGMT_VIEW	10	DEFAULT	
OE	10	DEFAULT	L
OLAPSYS	10	DEFAULT	L
ORDPLUGINS	10	DEFAULT	L
ORDSYS	10	DEFAULT	L
OUTLN	10	DEFAULT	L
PM	10	DEFAULT	L
SCOTT	4	PROFILE1	
SH	10	DEFAULT	L
SI_INFORMTN_SCHEMA	10	DEFAULT	L
SYS	10	DEFAULT	
SYSMAN	10	DEFAULT	
SYSTEM	10	DEFAULT	
TSMSYS	16	PROFILE3	L
USER1	10	DEFAULT	L
USER21	4	PROFILE1	
WMSYS	10	DEFAULT	L
XDB	10	DEFAULT	

2 users have unlimited failed login attempts allowed.

30 users have more than 6 failed login attempts allowed.

User accounts already locked are shown with an 'L'

2 PASSWORDS - Passwords

RISKS

In this section we look at password settings.

2.1 PWDCHNG - Password last changed

L

RISKS

This is the date the password was last changed. Passwords that are rarely changed soon become known to other people and segregation of users becomes weakened.

ACTIONS

Examine those users who have not changed there password recently, particularly any 'system' users.

H

RESULTS

Password last changed.

It is assumed that the input file was created on 11-Aug-2008

User	Change date	Days	Locked	
ANONYMOUS	30-Aug-2005	1077	L	
BI	02-Mar-2008	162	L	
CTXSYS	02-Mar-2008	162	L	
CXL_USER1	02-Mar-2008	162		<**
CXL_USER2	02-Mar-2008	162	L	
CXL_USER3	06-Mar-2008	158	L	
CXLUSER11	20-May-2008	83		
DAVE1				
DBSNMP	02-Mar-2008	162		<**
DIP	30-Aug-2005	1077	L	
DMSYS	30-Aug-2005	1077	L	
EXFSYS	30-Aug-2005	1077	L	
HR	02-Mar-2008	162	L	
IX	02-Mar-2008	162	L	
MDDATA	30-Aug-2005	1077	L	
MDSYS	30-Aug-2005	1077	L	
MGMT_VIEW	02-Mar-2008	162		<**
OE	02-Mar-2008	162	L	
OLAPSYS	30-Aug-2005	1077	L	
ORDPLUGINS	30-Aug-2005	1077	L	
ORDSYS	30-Aug-2005	1077	L	
OUTLN	30-Aug-2005	1077	L	
PM	02-Mar-2008	162	L	
SCOTT	30-Aug-2005	1077	L	
SH	02-Mar-2008	162	L	
SI_INFORMTN_SCHEMA	30-Aug-2005	1077	L	
SYS	02-Mar-2008	162		<**
SYSMAN	02-Mar-2008	162	L	
SYSTEM	11-Aug-2008	0		
TSMSYS	30-Aug-2005	1077	L	
USER1			L	
USER21	20-May-2008	83		
WMSYS	30-Aug-2005	1077	L	
XDB	30-Aug-2005	1077	L	

4 users have not changed their password recently.

2.2 PWDGRACE - Password grace time

L

RISKS

The number of days after the grace period begins during which a warning is issued and login is allowed. If the password is not changed during the grace period, the password expires

ACTIONS

This parameter should be set to a low number of days, less than 10.

RESULTS

Password grace time settings (days).

User	Setting	Profile
ANONYMOUS	22	DEFAULT
BI	22	DEFAULT
CTXSYS	22	DEFAULT
CXL_USER1	22	DEFAULT
CXL_USER2	6	PROFILE3
CXL_USER3	22	MONITORING_PROFILE
CXLUSER11	22	DEFAULT
DAVE1	22	DEFAULT
DBSNMP	22	MONITORING_PROFILE
DIP	22	DEFAULT
DMSYS	22	DEFAULT
EXFSYS	22	DEFAULT
HR	22	DEFAULT
IX	22	DEFAULT
MDDATA	22	DEFAULT
MDSYS	22	DEFAULT
MGMT_VIEW	22	DEFAULT
OE	22	DEFAULT
OLAPSYS	22	DEFAULT
ORDPLUGINS	22	DEFAULT
ORDSYS	22	DEFAULT
OUTLN	22	DEFAULT
PM	22	DEFAULT
SCOTT	22	PROFILE1
SH	22	DEFAULT
SI_INFORMTN_SCHEMA	22	DEFAULT
SYS	22	DEFAULT
SYSMAN	22	DEFAULT
SYSTEM	22	DEFAULT
TSMSYS	6	PROFILE3
USER1	22	DEFAULT
USER21	22	PROFILE1
WMSYS	22	DEFAULT
XDB	22	DEFAULT

No users have unlimited grace login times allowed.

32 users have more than 10 days grace login time allowed.

2.3 PWDLIFE - Password life time

RISKS

The number of days the same password can be used for authentication.

ACTIONS

This parameter should be set to your company standards and ideally be less than 60 days.

H

RESULTS

Password life time (days).

User	Setting	Profile
ANONYMOUS	77 *	DEFAULT *
BI	77 *	DEFAULT *
CTXSYS	77 *	DEFAULT *
CXL_USER1	77 *	DEFAULT *
CXL_USER2	99 *	PROFILE3 *
CXL_USER3	77 *	MONITORING_PROFILE *
CXLUSER11	77 *	DEFAULT *
DAVE1	77 *	DEFAULT *
DBSNMP	77 *	MONITORING_PROFILE *
DIP	77 *	DEFAULT *
DMSYS	77 *	DEFAULT *
EXFSYS	77 *	DEFAULT *
HR	77 *	DEFAULT *
IX	77 *	DEFAULT *
MDDATA	77 *	DEFAULT *
MDSYS	77 *	DEFAULT *
MGMT_VIEW	77 *	DEFAULT *
OE	77 *	DEFAULT *
OLAPSYS	77 *	DEFAULT *
ORDPLUGINS	77 *	DEFAULT *
ORDSYS	77 *	DEFAULT *
OUTLN	77 *	DEFAULT *
PM	77 *	DEFAULT *
SCOTT	77 *	PROFILE1 *
SH	77 *	DEFAULT *
SI_INFORMTN_SCHEMA	77 *	DEFAULT *
SYS	77 *	DEFAULT *
SYSMAN	77 *	DEFAULT *
SYSTEM	77 *	DEFAULT *
TSMSYS	99 *	PROFILE3 *
USER1	77 *	DEFAULT *
USER21	77 *	PROFILE1 *
WMSYS	77 *	DEFAULT *
XDB	77 *	DEFAULT *

No users have unlimited password life times allowed.

34 users have more than your policy password life minimum time allowed.

The policy setting for ordinary users is 60 days.
The policy setting for system users is 30 days.

2.4 PWDLOCK - Password lock time

L

RISKS

The number of days an account will be locked after the specified number of consecutive failed login attempts defined by FAILED_LOGIN_ATTEMPTS.
Setting this to unlimited means that the account can only be unlocked by the database administrator.

ACTIONS

This parameter should be set at least 15 minutes (0.04 days).

L

RESULTS

Password lock time settings (days).

User	Setting	Profile
ANONYMOUS	20	DEFAULT
BI	20	DEFAULT
CTXSYS	20	DEFAULT
CXL_USER1	20	DEFAULT
CXL_USER2	12	PROFILE3
CXL_USER3	20	MONITORING_PROFILE
CXLUSER11	20	DEFAULT
DAVE1	20	DEFAULT
DBSNMP	20	MONITORING_PROFILE
DIP	20	DEFAULT
DMSYS	20	DEFAULT
EXFSYS	20	DEFAULT
HR	20	DEFAULT
IX	20	DEFAULT
MDDATA	20	DEFAULT
MDSYS	20	DEFAULT
MGMT_VIEW	20	DEFAULT
OE	20	DEFAULT
OLAPSYS	20	DEFAULT
ORDPLUGINS	20	DEFAULT
ORDSYS	20	DEFAULT
OUTLN	20	DEFAULT
PM	20	DEFAULT
SCOTT	20	PROFILE1
SH	20	DEFAULT
SI_INFORMTN_SCHEMA	20	DEFAULT
SYS	20	DEFAULT
SYSMAN	20	DEFAULT
SYSTEM	20	DEFAULT
TSMSYS	12	PROFILE3
USER1	20	DEFAULT
USER21	20	PROFILE1
WMSYS	20	DEFAULT
XDB	20	DEFAULT

No users have unlimited password lock times allowed.

No users have less than 1 day password lock time allowed.

2.5 PWDREUSENO - Password reuse number

M

RISKS

This is the number of password changes that must occur before the password can be reused. Unlimited means that passwords can never be re-used.

ACTIONS

This parameter should be set to at least 20 before using the password again.

H

RESULTS

Password reuse number:

User	Setting	Profile
ANONYMOUS	UNLIMITED	DEFAULT
BI	UNLIMITED	DEFAULT
CTXSYS	UNLIMITED	DEFAULT
CXL_USER1	UNLIMITED	DEFAULT
CXL_USER2	22	PROFILE3
CXL_USER3	UNLIMITED	MONITORING_PROFILE
CXLUSER11	UNLIMITED	DEFAULT
DAVE1	UNLIMITED	DEFAULT
DBSNMP	UNLIMITED	MONITORING_PROFILE
DIP	UNLIMITED	DEFAULT
DMSYS	UNLIMITED	DEFAULT
EXFSYS	UNLIMITED	DEFAULT
HR	UNLIMITED	DEFAULT
IX	UNLIMITED	DEFAULT
MDDATA	UNLIMITED	DEFAULT
MDSYS	UNLIMITED	DEFAULT
MGMT_VIEW	UNLIMITED	DEFAULT
OE	UNLIMITED	DEFAULT
OLAPSYS	UNLIMITED	DEFAULT
ORDPLUGINS	UNLIMITED	DEFAULT
ORDSYS	UNLIMITED	DEFAULT
OUTLN	UNLIMITED	DEFAULT
PM	UNLIMITED	DEFAULT
SCOTT	7	PROFILE1
SH	UNLIMITED	DEFAULT
SI_INFORMTN_SCHEMA	UNLIMITED	DEFAULT
SYS	UNLIMITED	DEFAULT
SYSMAN	UNLIMITED	DEFAULT
SYSTEM	UNLIMITED	DEFAULT
TSMSYS	22	PROFILE3
USER1	UNLIMITED	DEFAULT
USER21	7	PROFILE1
WMSYS	UNLIMITED	DEFAULT
XDB	UNLIMITED	DEFAULT

30 users have unlimited password reuse.

32 users have less than 20 password changes required.

2.6 PWDREUSETIME - Password reuse time

M

RISKS

The number of days between reuses of a password.

ACTIONS

This parameter should be set to at least 200.

H

RESULTS

Password reuse time (days).

User	Setting	Profile
ANONYMOUS	60	DEFAULT
BI	60	DEFAULT
CTXSYS	60	DEFAULT
CXL_USER1	60	DEFAULT
CXL_USER2	56	PROFILE3
CXL_USER3	60	MONITORING_PROFILE
CXLUSER11	60	DEFAULT
DAVE1	60	DEFAULT
DBSNMP	60	MONITORING_PROFILE
DIP	60	DEFAULT
DMSYS	60	DEFAULT
EXFSYS	60	DEFAULT
HR	60	DEFAULT
IX	60	DEFAULT
MDDATA	60	DEFAULT
MDSYS	60	DEFAULT
MGMT_VIEW	60	DEFAULT
OE	60	DEFAULT
OLAPSYS	60	DEFAULT
ORDPLUGINS	60	DEFAULT
ORDSYS	60	DEFAULT
OUTLN	60	DEFAULT
PM	60	DEFAULT
SCOTT	60	PROFILE1
SH	60	DEFAULT
SI_INFORMTN_SCHEMA	60	DEFAULT
SYS	60	DEFAULT
SYSMAN	60	DEFAULT
SYSTEM	60	DEFAULT
TSMSYS	56	PROFILE3
USER1	60	DEFAULT
USER21	60	PROFILE1
WMSYS	60	DEFAULT
XDB	60	DEFAULT

No users are prevented from using old password.

34 users can reuse passwords within 200 days.

2.7 PWDVERIFY - Password verify function

L

RISKS

This specifies a function which is used to verify the password to ensure that it is strong and complex.
If set to NULL, no function is used.

ACTIONS

This should NOT be set to NULL and a verify function should be used.

H

RESULTS

```
Password verify function.

User                           Setting
------------------------------------------------------------------------
ANONYMOUS                      NULL
BI                             NULL
CTXSYS                         NULL
CXL_USER1                      NULL
CXL_USER2                      NULL
CXL_USER3                      NULL
CXLUSER11                      NULL
DAVE1                          NULL
DBSNMP                         NULL
DIP                            NULL
DMSYS                          NULL
EXFSYS                         NULL
HR                             NULL
IX                             NULL
MDDATA                         NULL
MDSYS                          NULL
MGMT_VIEW                      NULL
OE                             NULL
OLAPSYS                        NULL
ORDPLUGINS                     NULL
ORDSYS                         NULL
OUTLN                          NULL
PM                             NULL
SCOTT                          NULL
SH                             NULL
SI_INFORMTN_SCHEMA             NULL
SYS                            NULL
SYSMAN                         NULL
SYSTEM                         NULL
TSMSYS                         NULL
USER1                          NULL
USER21                         NULL
WMSYS                          NULL
XDB                            NULL

0 users employ a password verification function.
```

3 PROFILES - User profiles

RISKS

In this section we look at the user profile settings.

3.1 DEFPROF - The DEFAULT profile

L

RISKS

Each user has a profile and when they don't, the DEFAULT profile is applied. If the default profile has not been modified, many of its security settings will be set to UNLIMITED.
These will then be applied to users.

ACTIONS

Modify the DEFAULT profile so that all settings conform to the system policy.Create profiles for users based on their job function and set security appropriately.

H

RESULTS

```
The DEFAULT profile looks like this:
                                22
COMPOSITE_LIMIT                 1
CONNECT_TIME                    UNLIMITED
CPU_PER_CALL                    2
CPU_PER_SESSION                 UNLIMITED
FAILED_LOGIN_ATTEMPTS           10
IDLE_TIME                       5
LOGICAL_READS_PER_CALL          UNLIMITED
LOGICAL_READS_PER_SESSION       UNLIMITED
PASSWORD_GRACE_TIME             22
PASSWORD_LIFE_TIME              77
PASSWORD_LOCK_TIME              20
PASSWORD_REUSE_MAX              UNLIMITED
PASSWORD_REUSE_TIME             60
PASSWORD_VERIFY_FUNCTION        NULL
PRIVATE_SGA                     UNLIMITED
SESSIONS_PER_USER               UNLIMITED

The following users use the DEFAULT profile.
ANONYMOUS                       BI
CTXSYS                          CXL_USER1
CXLUSER11                       DAVE1
DIP                             DMSYS
EXFSYS                          HR
IX                              MDDATA
MDSYS                           MGMT_VIEW
OE                              OLAPSYS
ORDPLUGINS                      ORDSYS
OUTLN                           PM
SH                              SI_INFORMTN_SCHEMA
SYS                             SYSMAN
SYSTEM                          USER1
WMSYS                           XDB
```

3.2 OTHPROF - Other profiles

(L)

RISKS

Every user should be grouped into a profile which restricts their actions by means of the various security settings.

ACTIONS

Ensure that each profile is appropriate for the users duties.

(H)

RESULTS

```
The MONITORING_PROFILE profile:
                               22
COMPOSITE_LIMIT                1
CONNECT_TIME                   UNLIMITED
CPU_PER_CALL                   2
CPU_PER_SESSION                UNLIMITED
FAILED_LOGIN_ATTEMPTS          UNLIMITED
IDLE_TIME                      5
LOGICAL_READS_PER_CALL         UNLIMITED
LOGICAL_READS_PER_SESSION      UNLIMITED
PASSWORD_GRACE_TIME            22
PASSWORD_LIFE_TIME             77
PASSWORD_LOCK_TIME             20
PASSWORD_REUSE_MAX             UNLIMITED
PASSWORD_REUSE_TIME            60
PASSWORD_VERIFY_FUNCTION       NULL
PRIVATE_SGA                    UNLIMITED
SESSIONS_PER_USER              UNLIMITED

The following users use the MONITORING_PROFILE profile.
CXL_USER3                     DBSNMP


The PROFILE1 profile:
                               22
COMPOSITE_LIMIT                1
CONNECT_TIME                   UNLIMITED
CPU_PER_CALL                   2
CPU_PER_SESSION                UNLIMITED
FAILED_LOGIN_ATTEMPTS          4
IDLE_TIME                      5
LOGICAL_READS_PER_CALL         UNLIMITED
LOGICAL_READS_PER_SESSION      UNLIMITED
PASSWORD_GRACE_TIME            22
PASSWORD_LIFE_TIME             77
PASSWORD_LOCK_TIME             20
PASSWORD_REUSE_MAX             7
PASSWORD_REUSE_TIME            60
PASSWORD_VERIFY_FUNCTION       NULL
PRIVATE_SGA                    UNLIMITED
SESSIONS_PER_USER              UNLIMITED

The following users use the PROFILE1 profile.
SCOTT                          USER21


The PROFILE3 profile:
                               6
COMPOSITE_LIMIT                1
CONNECT_TIME                   UNLIMITED
CPU_PER_CALL                   UNLIMITED
CPU_PER_SESSION                7
FAILED_LOGIN_ATTEMPTS          16
IDLE_TIME                      5
LOGICAL_READS_PER_CALL         UNLIMITED
LOGICAL_READS_PER_SESSION      UNLIMITED
PASSWORD_GRACE_TIME            6
PASSWORD_LIFE_TIME             99
PASSWORD_LOCK_TIME             12
PASSWORD_REUSE_MAX             22
PASSWORD_REUSE_TIME            56
PASSWORD_VERIFY_FUNCTION       NULL
PRIVATE_SGA                    UNLIMITED
SESSIONS_PER_USER              UNLIMITED

The following users use the PROFILE3 profile.
CXL_USER2                     TSMSYS
```

4 PRIVILEGES - Privileges

RISKS

In this section we look at the system and object privileges available to users.

4.1 OSYSPRIV - User's system privileges

M

RISKS

System privileges give users the ability to perform actions on a database. Changes to the databases or the user's job will mean that managing the privileges can become very difficult.

ACTIONS

We recommend that privileges are not applied directly to user but instead are given to roles and the roles applied to the users.

L

RESULTS

```
User=BI
-------
ADVISOR                         ALTER ANY MATERIALIZED VIEW
ALTER ANY ROLE                  ALTER ANY TABLE
ALTER RESOURCE COST             CREATE ANY JOB
CREATE ANY OUTLINE              CREATE ANY SYNONYM
CREATE CLUSTER                  CREATE INDEXTYPE
CREATE OPERATOR                 CREATE PROCEDURE
CREATE SEQUENCE                 CREATE TABLE
CREATE TRIGGER                  CREATE TYPE

User=CTXSYS
-----------
ADVISOR                         ALTER ANY MATERIALIZED VIEW
ALTER ANY ROLE                  ALTER ANY TABLE
ALTER RESOURCE COST             CREATE ANY JOB
CREATE ANY OUTLINE              CREATE ANY SYNONYM
CREATE CLUSTER                  CREATE INDEXTYPE
CREATE OPERATOR                 CREATE PROCEDURE
CREATE SEQUENCE                 CREATE TABLE
CREATE TRIGGER                  CREATE TYPE

User=CXL_USER2
--------------
ADMINISTER ANY SQL TUNING SET ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER   ADMINISTER SQL TUNING SET
ADVISOR                         ALTER ANY CLUSTER
ALTER ANY DIMENSION             ALTER ANY EVALUATION CONTEXT
ALTER ANY INDEX                 ALTER ANY INDEXTYPE
ALTER ANY LIBRARY               ALTER ANY MATERIALIZED VIEW
ALTER ANY OUTLINE               ALTER ANY PROCEDURE
ALTER ANY ROLE                  ALTER ANY RULE
ALTER ANY RULE SET              ALTER ANY SEQUENCE
ALTER ANY SQL PROFILE           ALTER ANY TABLE
ALTER ANY TRIGGER               ALTER ANY TYPE
ALTER DATABASE                  ALTER PROFILE
ALTER RESOURCE COST             ALTER ROLLBACK SEGMENT
ALTER SESSION                   ALTER SYSTEM
ALTER TABLESPACE                ALTER USER
ANALYZE ANY                     ANALYZE ANY DICTIONARY
AUDIT ANY                       AUDIT SYSTEM
BACKUP ANY TABLE                BECOME USER
CHANGE NOTIFICATION             COMMENT ANY TABLE
CREATE ANY CLUSTER              CREATE ANY CONTEXT
CREATE ANY DIMENSION            CREATE ANY DIRECTORY
CREATE ANY EVALUATION CONTEXT CREATE ANY INDEX
CREATE ANY INDEXTYPE            CREATE ANY JOB
CREATE ANY LIBRARY              CREATE ANY MATERIALIZED VIEW
CREATE ANY OPERATOR             CREATE ANY OUTLINE
CREATE ANY PROCEDURE            CREATE ANY RULE
CREATE ANY RULE SET             CREATE ANY SEQUENCE
CREATE ANY SQL PROFILE          CREATE ANY SYNONYM
CREATE ANY TABLE                CREATE ANY TRIGGER
CREATE ANY TYPE                 CREATE ANY VIEW
CREATE CLUSTER                  CREATE DATABASE LINK
CREATE DIMENSION                CREATE EVALUATION CONTEXT
CREATE EXTERNAL JOB             CREATE INDEXTYPE
CREATE JOB                      CREATE LIBRARY
CREATE MATERIALIZED VIEW        CREATE OPERATOR
CREATE PROCEDURE                CREATE PROFILE
CREATE PUBLIC DATABASE LINK   CREATE PUBLIC SYNONYM
CREATE ROLE                     CREATE ROLLBACK SEGMENT
CREATE RULE                     CREATE RULE SET
CREATE SEQUENCE                 CREATE SESSION
CREATE SYNONYM                  CREATE TABLE
CREATE TABLESPACE               CREATE TRIGGER
CREATE TYPE                     CREATE USER
```

4.2 OPQUANY - Users with ANY privilege

M

RISKS

Privileges that contain the ANY keyword are usually high risk and can be applied to any chosen object.

ACTIONS

Examine the users shown below and decide if they really need these privileges.

H

RESULTS

User	Privilege	With Admin
BI	ALTER ANY MATERIALIZED VIEW	
BI	ALTER ANY ROLE	
BI	ALTER ANY TABLE	
BI	CREATE ANY JOB	
BI	CREATE ANY OUTLINE	
BI	CREATE ANY SYNONYM	
CTXSYS	ALTER ANY MATERIALIZED VIEW	
CTXSYS	ALTER ANY ROLE	
CTXSYS	ALTER ANY TABLE	
CTXSYS	CREATE ANY JOB	
CTXSYS	CREATE ANY OUTLINE	
CTXSYS	CREATE ANY SYNONYM	
CXL_USER2	ADMINISTER ANY SQL TUNING SET	
CXL_USER2	ALTER ANY CLUSTER	
CXL_USER2	ALTER ANY DIMENSION	
CXL_USER2	ALTER ANY EVALUATION CONTEXT	
CXL_USER2	ALTER ANY INDEX	
CXL_USER2	ALTER ANY INDEXTYPE	
CXL_USER2	ALTER ANY LIBRARY	
CXL_USER2	ALTER ANY MATERIALIZED VIEW	
CXL_USER2	ALTER ANY OUTLINE	
CXL_USER2	ALTER ANY PROCEDURE	
CXL_USER2	ALTER ANY ROLE	
CXL_USER2	ALTER ANY RULE	
CXL_USER2	ALTER ANY RULE SET	
CXL_USER2	ALTER ANY SEQUENCE	
CXL_USER2	ALTER ANY SQL PROFILE	
CXL_USER2	ALTER ANY TABLE	
CXL_USER2	ALTER ANY TRIGGER	
CXL_USER2	ALTER ANY TYPE	
CXL_USER2	ANALYZE ANY	
CXL_USER2	ANALYZE ANY DICTIONARY	
CXL_USER2	AUDIT ANY	
CXL_USER2	BACKUP ANY TABLE	
CXL_USER2	COMMENT ANY TABLE	
CXL_USER2	CREATE ANY CLUSTER	
CXL_USER2	CREATE ANY CONTEXT	
CXL_USER2	CREATE ANY DIMENSION	
CXL_USER2	CREATE ANY DIRECTORY	
CXL_USER2	CREATE ANY EVALUATION CONTEXT	
CXL_USER2	CREATE ANY INDEX	
CXL_USER2	CREATE ANY INDEXTYPE	
CXL_USER2	CREATE ANY JOB	
CXL_USER2	CREATE ANY LIBRARY	
CXL_USER2	CREATE ANY MATERIALIZED VIEW	
CXL_USER2	CREATE ANY OPERATOR	
CXL_USER2	CREATE ANY OUTLINE	
CXL_USER2	CREATE ANY PROCEDURE	
CXL_USER2	CREATE ANY RULE	
CXL_USER2	CREATE ANY RULE SET	
CXL_USER2	CREATE ANY SEQUENCE	
CXL_USER2	CREATE ANY SQL PROFILE	
CXL_USER2	CREATE ANY SYNONYM	
CXL_USER2	CREATE ANY TABLE	
CXL_USER2	CREATE ANY TRIGGER	
CXL_USER2	CREATE ANY TYPE	
CXL_USER2	CREATE ANY VIEW	
CXL_USER2	DEBUG ANY PROCEDURE	
CXL_USER2	DELETE ANY TABLE	
CXL_USER2	DEQUEUE ANY QUEUE	
CXL_USER2	DROP ANY CLUSTER	
CXL_USER2	DROP ANY CONTEXT	
CXL_USER2	DROP ANY DIMENSION	
CXL_USER2	DROP ANY DIRECTORY	
CXL_USER2	DROP ANY EVALUATION CONTEXT	
CXL_USER2	DROP ANY INDEX	

5 ROLES - Roles

RISKS

In this section we look at some of the user settings which effect the security of the system.

5.1 OROLDBA - Users granted the DBA Role

H

RISKS

The DBA role is the most powerful standard role available and has lots of privileges. It should only be applied to certain dtatbase administrators.

ACTIONS

Examine the users shown below and decide if they really need this role.

M

RESULTS

```
The following users have the DBA role.
--------------------------------------

CXL_USER2                      CXL_USER3                      PUBLIC
```

5.2 OROLANY - Roles with ANY privilege

M

RISKS

Privileges that contain the ANY keyword are usually high risk and can be applied to any chosen object.

ACTIONS

Examine the users shown below and decide if they really need these privileges.

H

RESULTS

Role	Privilege	With Admin
AQ_ADMINISTRATOR_ROLE	DEQUEUE ANY QUEUE	
AQ_ADMINISTRATOR_ROLE	ENQUEUE ANY QUEUE	
AQ_ADMINISTRATOR_ROLE	MANAGE ANY QUEUE	
EXP_FULL_DATABASE	BACKUP ANY TABLE	
EXP_FULL_DATABASE	EXECUTE ANY PROCEDURE	
EXP_FULL_DATABASE	EXECUTE ANY TYPE	
EXP_FULL_DATABASE	READ ANY FILE GROUP	
EXP_FULL_DATABASE	SELECT ANY SEQUENCE	
EXP_FULL_DATABASE	SELECT ANY TABLE	
IMP_FULL_DATABASE	ALTER ANY PROCEDURE	
IMP_FULL_DATABASE	ALTER ANY TABLE	
IMP_FULL_DATABASE	ALTER ANY TRIGGER	
IMP_FULL_DATABASE	ALTER ANY TYPE	
IMP_FULL_DATABASE	ANALYZE ANY	
IMP_FULL_DATABASE	AUDIT ANY	
IMP_FULL_DATABASE	COMMENT ANY TABLE	
IMP_FULL_DATABASE	CREATE ANY CLUSTER	
IMP_FULL_DATABASE	CREATE ANY CONTEXT	
IMP_FULL_DATABASE	CREATE ANY DIMENSION	
IMP_FULL_DATABASE	CREATE ANY DIRECTORY	
IMP_FULL_DATABASE	CREATE ANY INDEX	
IMP_FULL_DATABASE	CREATE ANY INDEXTYPE	
IMP_FULL_DATABASE	CREATE ANY LIBRARY	
IMP_FULL_DATABASE	CREATE ANY MATERIALIZED VIEW	
IMP_FULL_DATABASE	CREATE ANY OPERATOR	
IMP_FULL_DATABASE	CREATE ANY PROCEDURE	
IMP_FULL_DATABASE	CREATE ANY SEQUENCE	
IMP_FULL_DATABASE	CREATE ANY SQL PROFILE	
IMP_FULL_DATABASE	CREATE ANY SYNONYM	
IMP_FULL_DATABASE	CREATE ANY TABLE	
IMP_FULL_DATABASE	CREATE ANY TRIGGER	
IMP_FULL_DATABASE	CREATE ANY TYPE	
IMP_FULL_DATABASE	CREATE ANY VIEW	
IMP_FULL_DATABASE	DROP ANY CLUSTER	
IMP_FULL_DATABASE	DROP ANY CONTEXT	
IMP_FULL_DATABASE	DROP ANY DIMENSION	
IMP_FULL_DATABASE	DROP ANY DIRECTORY	
IMP_FULL_DATABASE	DROP ANY INDEX	
IMP_FULL_DATABASE	DROP ANY INDEXTYPE	
IMP_FULL_DATABASE	DROP ANY LIBRARY	
IMP_FULL_DATABASE	DROP ANY MATERIALIZED VIEW	
IMP_FULL_DATABASE	DROP ANY OPERATOR	
IMP_FULL_DATABASE	DROP ANY OUTLINE	
IMP_FULL_DATABASE	DROP ANY PROCEDURE	
IMP_FULL_DATABASE	DROP ANY ROLE	
IMP_FULL_DATABASE	DROP ANY SEQUENCE	
IMP_FULL_DATABASE	DROP ANY SQL PROFILE	
IMP_FULL_DATABASE	DROP ANY SYNONYM	
IMP_FULL_DATABASE	DROP ANY TABLE	
IMP_FULL_DATABASE	DROP ANY TRIGGER	
IMP_FULL_DATABASE	DROP ANY TYPE	
IMP_FULL_DATABASE	DROP ANY VIEW	
IMP_FULL_DATABASE	EXECUTE ANY PROCEDURE	
IMP_FULL_DATABASE	EXECUTE ANY TYPE	
IMP_FULL_DATABASE	INSERT ANY TABLE	
IMP_FULL_DATABASE	MANAGE ANY QUEUE	
IMP_FULL_DATABASE	SELECT ANY TABLE	
IMP_FULL_DATABASE	UPDATE ANY TABLE	
JAVADEBUGPRIV	DEBUG ANY PROCEDURE	
OEM_MONITOR	ANALYZE ANY	
OEM_MONITOR	ANALYZE ANY DICTIONARY	
OEM_MONITOR	MANAGE ANY QUEUE	
OEM_MONITOR	SELECT ANY DICTIONARY	
OLAP_DBA	ALTER ANY DIMENSION	
OLAP_DBA	ALTER ANY TABLE	
OLAP_DBA	ANALYZE ANY	

5.3 OROLPWD - Roles without passwords

L

RISKS

Where a role has important privileges attached to it, these roles should need a password to access them.
These roles do not require a password.

ACTIONS

Examine any sensitive roles and ensure that they are password protected.

H

RESULTS

```
The following roles do not have passwords.
------------------------------------------

AQ_ADMINISTRATOR_ROLE          AQ_USER_ROLE
AUTHENTICATEDUSER              CTXAPP
CXL1                           DBA
DELETE_CATALOG_ROLE            EJBCLIENT
EXECUTE_CATALOG_ROLE           EXP_FULL_DATABASE
GATHER_SYSTEM_STATISTICS       HS_ADMIN_ROLE
IMP_FULL_DATABASE              JAVA_ADMIN
JAVA_DEPLOY                    JAVADEBUGPRIV
JAVAIDPRIV                     JAVASYSPRIV
JAVAUSERPRIV                   LOGSTDBY_ADMINISTRATOR
MGMT_USER                      MYROLE1
OEM_MONITOR                    OLAP_DBA
OLAP_USER                      RECOVERY_CATALOG_OWNER
RESOURCE                       ROLE9
SCHEDULER_ADMIN                SELECT_CATALOG_ROLE
WM_ADMIN_ROLE                  XDBADMIN
XDBWEBSERVICES
```

5.4 OROLPUB - Roles granted to PUBLIC

M

RISKS

Roles, and their associated privileges will be granted to every user of the database.

ACTIONS

Remove the roles from PUBLIC and assign roles to users instead.

L

RESULTS

6 SYSTEM - System settings

RISKS

In this section we look at the system settings.

6.1 SYSLOGPWDFILE - Remote login password file

M

RISKS

The parameter 'remote_login_passwordfile' specifies if Oracle checks for a password file and if this password file is shared among databases.
Settings:
None - Oracle ignores the password file if it exists.
Exclusive - Password file is exclusively used by one database.
Internal - Used for Oracle Parallel Server
Shared - The password file is shared among databases. However, the only users that can be authenticated are sys (and obsoletly: internal). If the password file is shared, only SYS can be added to the password file.

ACTIONS

Recommended value is 'Exclusive'.

L

RESULTS

```
The 'remote_login_passwordfile' parameter is set to EXCLUSIVE
Password file is exclusively used by one database.
```

6.2 SYSOSAUTH - Remote OS authentication

H

RISKS

TRUE allows operating system authentication over a non-secure connection and can allow a user to impersonate another operating system user and connect to the database without having to supply a password.

ACTIONS

Recommended value: FALSE

L

RESULTS

```
The 'remote_os_authent' parameter is set to FALSE
Operating system authentication over a non-secure connection is NOT allowed.
```

6.3 SYSDATADIC - Data dictionary Accessibility

M

RISKS

This parameter, when set to false, prevents the privilege SELECT ANY TABLE from selecting system data tables.

ACTIONS

Recommended value: FALSE

L

RESULTS

```
The current setting for this parameter is FALSE.
```