



**Deloitte.**



# LEADING PRACTICES IN DATABASE AUDITING

**August 31, 2010**

Victoria Tudor  
Advisory Manager  
Deloitte & Touche LLP  
vtudor@deloitte.com

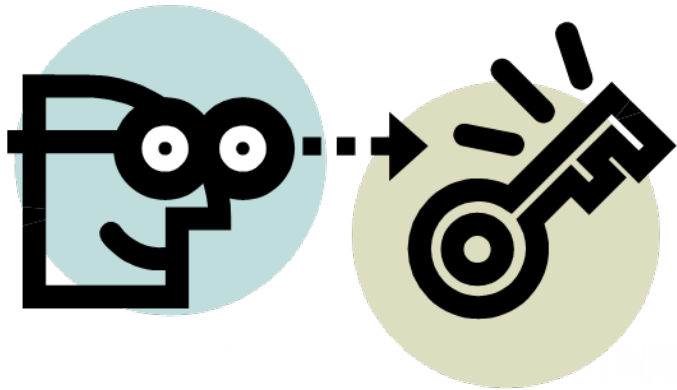
Audit • Tax • Consulting • Financial Advisory.

# Agenda

---

- Introduction
- Scoping
- Application/ Generic accounts
- Highlights from SQL and Oracle auditing
- Questions

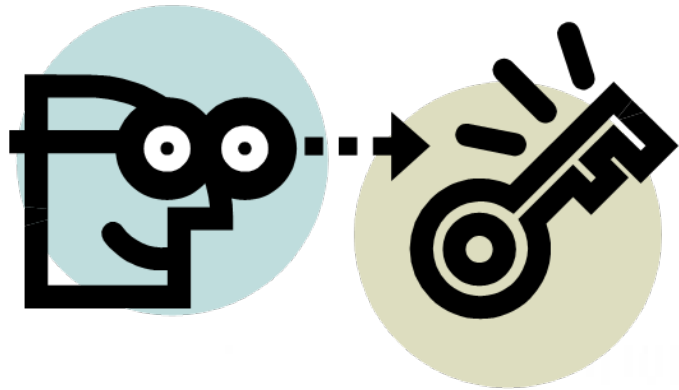
# Gain an understanding of the Database environment



- Type, Version and release of the Database
- Version and release of the underlying operating system
- Number of database instances
- Applications and related versions accessing the database (e.g. ERP, web, custom)
- Utilities used to logon and manage the database, Identity management software, monitoring packages
- Copies of the organization's key security policies and standards
- Organization charts identifying system owners and maintainers
- Outstanding audit findings, if any, from previous years

# Data Gathering

---



- Using auditing products (SekChek, etc)
- Using auditor provided scripts
- Using client scripts / SQL
- Using GUI

# Common SOX Controls

---

1. Database Security policies exist and are up-to-date
2. New database access is approved
3. Access of terminated and/or transferred employees is removed timely
4. Default vendor passwords are changed
5. Direct database modify access is limited based on job responsibilities and is subject to corporate password policies
  - User access
  - Application access (generic/system ID access)

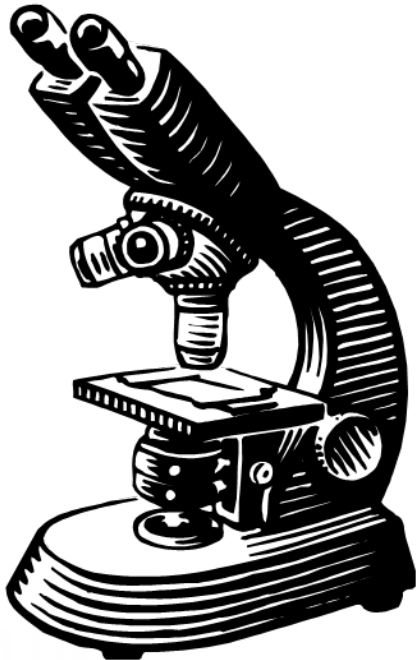
## **AUDIT CONSIDERATIONS:**

Common mitigating detective control:

*All successful logins to accounts with authority to modify data are logged and reviewed.*

# Database Audit Scope- Sarbanes Oxley

---



- Direct access to modify (Add, Change & Delete) data
  - In-scope Access - access that allows someone to login to the database directly, bypass application controls, and **MODIFY** data

## **AUDIT CONSIDERATIONS:**

Depending on the data stored in the database, “Read” access may be important. For example, confidential personal information in the HR database; trade secrets; credentials, etc  
PCI compliance also focuses on data protection.

# Identifying In-Scope Accounts

---

- Individual account permissions
  - Grant User A access to update Customer Contract table
- Role based or group based account permissions
  - Grant User B CustomerSupport Role
  - Grant CustomerSupport Role access to update Customer Contract table

## **AUDIT CONSIDERATIONS:**

Individual account permissions can be granted in addition to role based access:  
Grant User A Customer-Read-only role  
Grant User A access to update Customer Contract table

Naming rules are flexible:

Grant User B Customer-Read-only Role  
Grant Customer-Read-only Role access to update Customer Contract table

# Application or Generic ID Access

---



# Understanding Database Connections - Application

---

- Understand how an application communicates to its database
  - When user performs an action within the application (logs in, creates a document, etc), how does the database see it?

**Common practice:** Application uses generic account to connect to the database and perform tasks initiated by a user. User ID may be passed to the database but is not used to log in.

## **AUDIT CONSIDERATIONS:**

Application ID may have super user (MODIFY ALL) authority for all tables  
Password may be stored somewhere on the application or database server  
Password may be hardcoded into the application  
Password may not be encrypted or changed periodically  
Distinguishing between legitimate and illegitimate application log-ins and activity may be difficult  
Auditor would expect to see only DBAs and application IDs in the database

# Understanding Database Connections-Application (Continued)

- Understand how an application communicates to its database

**Common practice:** Application uses individual user accounts to connect to the database and perform tasks initiated by the user.

## **AUDIT CONSIDERATIONS:**

Individual users may be able to log in to the database directly

Individual users may have more authority in the database than in the application

Common password maybe used for every user and may not be compliant with company's password policies

Database may need to be kept up-to-date with new hires, transfers, and terminations

Distinguishing between direct database logins and logins through the application may be difficult

Mitigating controls may exist for User Account access

Auditor would expect to see DBAs and User Accounts in the database

# Understanding Database Connections - Interfaces

---

- Understand if there are other applications or databases that communicate with our target database (interfaces)
  - What's the nature of required interfaces? What level of access is needed?

## **AUDIT CONSIDERATIONS:**

Interface accounts may have more authority than they need

Passwords may be stored or hardcoded somewhere

Interface passwords may be replicated into development environment

It is difficult to determine where passwords are located and how many such locations exist

Passwords may not be changed periodically and may not be in compliance with company's password policies



# Identify Oracle SUPERUSERS

- 1) **SYS, SYSTEM**
- 2) **Users with access to ORACLE UNIX Account and accounts in the UNIX DBA group. These accounts may be able to enter the database as a SUPERUSER without additional authentication**
- 3) **All accounts that have 'UPDATE ANY TABLE','INSERT ANY TABLE','DELETE ANY TABLE' either individually or through a role**

## SAMPLE QUERY #1:

```
SQL> select grantee,privilege from dba_sys_privs where  
2 privilege in('UPDATE ANY TABLE','INSERT ANY TABLE','DELETE ANY TABLE')  
3 and grantee not in ('SYS','SYSTEM')  
4 ORDER BY grantee,privilege;
```

## SAMPLE OUTPUT #1:

### GRANTEE

-----  
DBA

IMP\_FULL\_DATABASE

apps

### PRIVILEGE

-----  
DELETE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE  
DELETE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE

# Identify SUPERUSERS (Continued)

Obtain the list of roles and accounts with these roles:

## SAMPLE QUERY #2:

```
SQL> select granted_role,grantee
2  from dba_role_privs
3  where granted_role not
4  in('CONNECT','RESOURCE')
5  order by 1
/
```

## SAMPLE OUTPUT #2:

GRANTED_ROLE	GRANTEE
DBA	SYS SYSTEM dba1 dba2
IMP_FULL_DATABASE	DBA
SELECT_CREDIT_ROLE	finuser1 finuser2





## Identify SUPERUSERS (Continued)

### QUERY #1 OUTPUT:

GRANTEE

DBA  
IMP\_FULL\_DATABASE  
apps

PRIVILEGE

DELETE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE  
DELETE ANY TABLE  
INSERT ANY TABLE  
UPDATE ANY TABLE

### QUERY #2 OUTPUT:

GRANTED\_ROLE

DBA

IMP\_FULL\_DATABASE  
SELECT\_CREDIT\_ROLE

GRANTEE

SYS  
SYSTEM  
dba1  
dba2  
DBA  
finuser1  
finuser2

### AUDIT CONSIDERATIONS:

The Following IDs are our "Superusers"

- SYS, SYSTEM, DBA1, DBA2, APPS

# Identify Access to Modify Data

List of accounts that have 'UPDATE ','INSERT','DELETE' access to modify tables either individually or through a role

## SAMPLE QUERY #1:

```
SQL> select table_name,owner,grantee,privilege from dba_tab_privs
2  where GRANTEE NOT IN('SYS','SYSTEM')
3  AND GRANTEE NOT IN(select distinct (GRANTEE) from dba_sys_privs
4  where privilege in('UPDATE ANY TABLE','INSERT ANY TABLE','DELETE ANY TABLE'))
5  AND privilege in('INSERT', 'DELETE', 'UPDATE')
6  order by table_name
7 /
```

## SAMPLE OUTPUT #1:

TABLE_NAME	OWNER	GRANTEE	PRIVILEGE
CUSTOMER	APPS	SELECT_CREDIT_ROLE	DELETE UPDATE INSERT
	APPS	GL_APP	DELETE UPDATE INSERT

## Identify Access to Modify Data (Continued)

Obtain the list of roles and accounts with these roles:

### SAMPLE QUERY #2:

```
SQL> select granted_role,grantee
       2  from dba_role_privs
       3  where granted_role not in('CONNECT','RESOURCE')
       4  order by 1
       5  /
```

### SAMPLE OUTPUT #2:

GRANTED_ROLE	GRANTEE
DBA	SYS SYSTEM dba1 dba2
IMP_FULL_DATABASE	DBA
SELECT_CREDIT_ROLE	finuser1 finuser2

### AUDIT CONSIDERATIONS:

The following IDs can modify CUSTOMER table:  
Finuser1, finuser2, GL\_APP

# Default Vendor Passwords

---

## Compare passwords to Oracle default password list

- Two user accounts are automatically created with the database and granted the DBA role. These two user accounts are:
  - **SYS** (initial password: **CHANGE\_ON\_INSTALL**)
  - **SYSTEM** (initial password: **MANAGER**)
- Default accounts will vary based on Oracle DB version & OF modules running
- For a full listing, refer to additional resources:
  - Patch 4943798 contains a SQL script that will list all open accounts with default password in your database
  - Starting with Oracle Database 11g, security administrators can check for default passwords by using the new database view `DBA_USERS_WITH_DEF_PWD`
  - [http://www.petefinnigan.com/default/default\\_password\\_list.htm](http://www.petefinnigan.com/default/default_password_list.htm)

## Default Vendor Passwords (Continued)

---

### SAMPLE QUERY:

```
SELECT 'user: SYS password is the default (CHANGE_ON_INSTALL/D4C5016086B2DC6A)' "default  
password", 'account status: ' || account_status  
FROM dba_users WHERE username='SYS' AND password='D4C5016086B2DC6A';
```

### SAMPLE OUTPUT:

- no rows selected

### AUDIT CONSIDERATIONS:

If default passwords are identified, we need to understand if accounts are open or locked

If default passwords are identified, we need to understand what risk the account poses

# Generic Application Account Access

---

1. Confirm with data owners that generic application account access is based on a valid business need
2. Identify who knows passwords of these generic application accounts and who has access to locations where such passwords are stored
3. Identify how often these passwords are changed and validate using a query (previously discussed)

**Accounts:** SYS, SYSTEM, APPS, GL\_APP

## **AUDIT CONSIDERATIONS:**

Password to **APPS** account may be stored in the following files:

iAS\_TOP/Apache/modplsql/cfg/wdbsvr.app

ORACLE\_HOME/reports60/server/CGIcmd.dat

NOTE: Search by name as a path may vary

DB\_Links in DEVELOPMENT DATABASES corresponding to production database may contain production passwords

SAMPLE QUERY: select \* from dba\_db\_links;

# SQL Access and permissions

---

- Individual account access
- Role Based Access
- Statement permissions restrict who can execute statements such as CREATE DATABASE, CREATE TABLE, or CREATE FUNCTION.
- Object permissions restrict access to objects such as tables, views, user-defined functions or stored procedures.

## **AUDIT CONSIDERATIONS:**

If there is a limited number of accounts, it may be easier to observe account permissions online with the DBA

The permissions system is based on the additive model. If user is in several groups, he adds all these permissions. However, as with Windows, if a particular role of which the user is a member has been denied a specific object permission (such as UPDATE), the user is unable to exercise that permission. The most restrictive permission (DENY) takes precedence.

# SQL Server Password Settings

---

- SA is a superuser account with default password of NULL
- SQL Server default password parameters are weak
- Application generic accounts may need to be controlled manually
  - Passwords need to be changed periodically and on as needed basis
  - Strong complex passwords should be used
  - Passwords should be available to DBAs only
- Guest account should be disabled;

## SAMPLE QUERY:

- All null passwords
  - Select name from sys.sql\_logins  
where pwdcompare("",password\_hash)=1; [or sysxlogins table ]
- Last password change date on SQL accounts
  - Select name, loginproperty(name, 'PasswordLastSetTime') from sys.sql\_logins

# Default SQL Server Roles

---

- **Sysadmin** Performs any activity in SQL Server
- **Serveradmin** Configures server-wide configuration options, shuts down the server
- **Setupadmin** Adds and removes linked servers, and executes some system stored procedures
- **Securityadmin** Manages server-wide security settings, including linked servers, and CREATE DATABASE permissions. Resets passwords for SQL Server authentication logins
- **Processadmin** Terminates processes running in SQL Server
- **Dbcreator** Creates, alters, drops, and restores any database
- **Diskadmin** Manages disk files
- **Bulkadmin** Allows a non-sysadmin user to run the **bulkadmin** statement

## **AUDIT CONSIDERATIONS:**

All members of the Windows BUILTIN\Administrators group (the local administrator's group) are members of the sysadmin role by default

# Default SQL Database Roles

---

- **db\_owner** Performs all maintenance and configuration activities in the database.
- **db\_accessadmin** Adds or removes access for Windows users, groups, and SQL Server logins.
- **db\_datareader** Reads all data from all user tables.
- **db\_datawriter** Adds, deletes, or changes data in all user tables.
- **db\_ddladmin** Runs any Data Definition Language (DDL) command in a database.
- **db\_securityadmin** Modifies role membership and manages permissions.
- **db\_backupoperator** Backs up the database.
- **db\_denydatareader** Cannot read any data in user tables within a database.
- **db\_denydatawriter** Cannot add, modify, or delete data in any user tables or views.

## **AUDIT CONSIDERATIONS:**

The PUBLIC role exists in every database. The PUBLIC role provides the default permissions for users in a database and cannot be deleted. Every database user is a member of this role automatically; therefore, users cannot be added or removed from this role.

In SQLServer DBAs can not change default roles( such as give db\_datareader more than read only access ) BUT can give PUBLIC more access.

# References and Resources

---

- <http://technet.microsoft.com/en-us/cc984178.aspx>
- “Oracle Database Security Checklist,” *An Oracle White Paper June 2008*
- <http://www.techonthenet.com/oracle/index.php>
- [http://www.petefinnigan.com/default/default\\_password\\_list.htm](http://www.petefinnigan.com/default/default_password_list.htm)

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the member firm of Deloitte Touche Tohmatsu, and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, and their subsidiaries) and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's website at [www.deloitte.com/us](http://www.deloitte.com/us).