If SOX is for the US only, then what's the non-US Oracle DBA got to do with it?

Suhas Upadhye
FannieMae

Session # 308

Speaker Qualifications

- Suhas Upadhye – Sr. DBA, FannieMae
- Suhas is an Oracle10g Certified Professional.
- Suhas possesses 8+ years hands-on experience in 'process' and 'data' modeling areas, data definition (meta-data), and other data management skills.
- Overall, 15+ years experience as a Systems Analyst and Programmer in Internet and Client/Server implementations.

Introduction: What is SOX?

- The **Public Company Accounting Reform and Investor Protection Act of 2002** (often called the Sarbanes Oxley Act, SOX, or SarbOX) implemented sweeping reforms to financial reporting in response to high profile scandals and bankruptcies such as WorldCom, Tyco International and Enron.

- The Act established a public company accounting oversight board, auditor independence, corporate responsibility and enhanced financial disclosure. It also granted the Securities and Exchange Commission (SEC) enhanced oversight authority.

- Pre-SOX, business was regulated largely by independent public accountants based on guidance from SEC. The accountants themselves established the auditing standards.

Non-US companies – Out-SOXed?

- Recent Reports:
  - Many European countries whose shares were traded in the U.S. were very ill-prepared to meet the deadlines of SOX
  - Compliance appeared to be an overwhelming task, especially when one considers that European companies have their own very specific regulations with which to concern themselves.
  - Outcry of criticism from Europe directed at the compliance provisions of SOX.
  - Possibility of overseas companies seeking to get de-listed from the US-exchanges.
  - BUT -- there is a decades-old SEC provision that states that if a foreign company has 300 or more shareholders in the United States, it cannot delist from the U.S. exchange where it is traded.

Non-US companies – Out-SOXed?

- Recent Reports:
  - Hence, SEC is ready to accommodate Europe – but should it?
  - Europe outstripped the US as a venue for stock market flotations for the first time last year, as companies sought refuge from the accounting requirements of America's Sarbanes-Oxley law.
  - In a dramatic reversal of historic norms, the money raised from IPOs in Europe almost doubled to €50bn in 2005, while US floats fell to just €27bn, according to PricewaterhouseCoopers.
  - The 8th EU Directive - *No SOX for Europe -- The Shaping of Controls Lies in Companies' Own Hands*

What are Business Benefits of SOX?

- European legislation is likely. SOX compliance means you are ahead
- SOX compliant companies are:
  - ready for US listing
  - ready for US acquisition
- Lower annual audit costs

Sarbanes-Oxley Brings Business Benefits Outside the USA

- Inventory of IT Assets - what, where and who owns it?
- What is Outsourced?
- Security - who has access? Is there an audit trail ?
- What IT Governance framework do you use? Is is similar to your peers?
- Data Transfers - how does your interoperability and data integrity work?
- Have you deployed ERP to replace other disparate systems? Should you do so?
- Do you have control of, have you eliminated end user spreadsheets?
- Are the systems tested for sustained SOX compliance requirements?
- Are you using SOX investment to consolidate IT systems?
- Are you using SOX investment for business process management and other reporting?

SOX : Standards setting bodies?

- **American Institute of Certified Public Accountants** (AICPA)

  Between 1938 and 1959, its Committee on Accounting Procedure (CAP) issued fifty-one authoritative pronouncements known as Accounting Research Bulletins that formed the basis of what became known as generally accepted accounting principles, or GAAP.

- **Financial Accounting Standards Board** (FASB)

  In 1972, FASB began to set the ground rules for measuring, reporting, and disclosing information in financial statements of non-governmental entities.

SOX Compliance

The goal of SOX is *improved accuracy and "transparency"* – to make the reporting of complex financial transactions more straightforward and obvious.

Overview of Privacy Statutes

FTC

HIPAA

Patriot Act

SOX

Privacy

GLB

FACT

DFARS: DoD Regulations

SEC Regulations

Summary of SOX provisions

- *Certification of financial reports by chief executive officers and chief financial officers*
- Ban on personal loans to any Executive Officer and Director
- Accelerated reporting of trades by insiders
- Prohibition on insider trades during pension fund blackout periods
- Public reporting of CEO and CFO compensation and profits
- *Additional disclosure*
- *Auditor independence, including outright bans on certain types of work and pre-certification by the company's Audit Committee of all other non-audit work*.

SOX Controls

- Protections are established via “controls”.

  These are processes intended to ensure the accuracy, timeliness, and completeness of financial data as well as compliance with policies and regulations. In addition, financial controls help to prevent or detect erroneous or inappropriate transactions. These standards involve people performing certain procedures, computer controls and monitoring reports.

- SOX Section 404 requires public companies to assess and report on the effectiveness of internal controls over financial reporting and requires the company's external audit firm to express an opinion on management’s assessment and to perform its own audit on the effectiveness of internal controls over financial reporting.

Control Examples

- **Separation of duties**
  - The person who controls the asset shouldn't be the person who accounts for it.
  - The person who executes the transaction shouldn't be the person who authorizes/approves it.
- **Procedures for initiating and approving transactions**. *Proper authorizations help to ensure that resources are expended appropriately*.

Control Examples

- **Maintaining adequate documents and records**
  - Ability to trace the transaction from the source document to the General Ledger and back again
  - Corporate chart of accounts -- basis for determining how financial information is organized and presented
- **Establishing physical control over assets and records**
  - Applications to track financial information
  - Locked file cabinets

Oracle Audit : Setup

- *Sox Auditor : Are the critical files on Oracle Installation protected sufficiently?*
- The critical files are the following and more...
  - Listener.ora -- could contain Listener password in clear text
  - spfileSID.ora -- contains accessible init.ora parameters
  - Backups *.dmp -- full backups contain Oracle hashkeys and dblink passwords in clear text

ALTER SESSION and ALTER SYSTEM

- *SOX Auditor: Which users have Alter Session and Alter System privs?*
- Two privileges that could essentially cripple the systems availability.

```
myoracle. me> select grantee, privilege, admin_option from dba_sys_privs
  2  where privilege in ('ALTER SYSTEM', 'ALTER SESSION', 'RESTRICTED SESSION');

GRANTEE                        PRIVILEGE                                ADM
------------------------------ ---------------------------------------- ---
DBA                            ALTER SYSTEM                             YES
DBA                            ALTER SESSION                            YES
DBA                            RESTRICTED SESSION                       YES
ORACLE                         ALTER SYSTEM                             NO
CONNECT                        ALTER SESSION                            NO
APPL_DBA_ROLE                  ALTER SESSION                            NO
LOWER_LEVEL_DBA                ALTER SESSION                            NO
RECOVERY_CATALOG_OWNER         ALTER SESSION                            NO

8 rows selected.
```

SYSTEM tablespace

- *SOX Auditor: Do you have any users who are using the SYSTEM tablespace?*

```
select username, default_tablespace, temporary_tablespace from dba_users
where default_tablespace= 'SYSTEM'
or temporary_tablespace = 'SYSTEM';

USERNAME                       DEFAULT_TABLESPACE             TEMPORARY_TABLESPACE
------------------------------ ------------------------------ --------------------
DBSNMP                         SYSTEM                         SYSTEM
OUTLN                          SYSTEM                         SYSTEM
SYS                            SYSTEM                         DSMTEMP
SYSTEM                         SYSTEM                         DSMTEMP
EDBAR                          SYSTEM                         DSMTEMP

Change them:
•    alter user dbsnmp default tablespace tools temporary tablespace DSMTEMP;
```

Listener

- *SOX Auditor: Can the Listener be compromised?*
  - Disable Online Modification of Listener – this will force va;ues to be changed in LISTENER.ORA and then Listener reloaded.

```
ADMIN_RESTRICTIONS_<ListenerNAme>=ON
```

  - Set a Listener Password

```
LSNRCTL> change_password
LSNRCTL> save_config
```

  - Disable OS Auhentication (10g) – undocumented parameter.

```
LOCAL_OS_AUTHENTICATION_<ListenerName>=OFF
```

DB-Links

- *Are the import/export logs secure?*
- Note that the import logs can show db-link passwords in plain text.

```
IMP-00015: following statement failed because the object already exists:
 "CREATE DATABASE LINK "AE2.PUT1S1" CONNECT TO "prod" IDENTIFIED BY
    "Fabu06" USING 'PGM19'"
IMP-00015: following statement failed because the object already exists:
 "CREATE DATABASE LINK "FCOS.TAE1S3" CONNECT TO "admp" IDENTIFIED BY
    “snowy1" USING 'OWR6'"
IMP-00015: following statement failed because the object already exists:
 "CREATE DATABASE LINK "Pascal1.WORLD" CONNECT TO "DevilD" IDENTIFIED BY
    "Fresco6" USING 'O_O0'"
```

Data Compliance Monitoring: Discovery

- *Sox Auditor: Are the pertinent database activities captured?*
- **Who** - identification of the person viewing or modifying the data
- **Where** - specific application procedure / method used to access the data
- **When** - time stamp of activities
- **What** - full listing of all activities

Detection & Prevention of Malicious and Misuse Activities

- Detect unauthorized database activities and prevent access of audit trail repository by DBA and System Administrators
- Ensure Application ID and User ID accessing database servers outside of the application is controlled
- Prevent rogue access to the database server over the network

Items Learned in this Session

- SOX terms and terminologies
- SOX Control examples
- SOX Auditor Q&A
- Basic SQL for data governance
- SOX is not there to punish but to guide
- SOX Compliance – always a work-in-progress
- SOX makes common(security)sence – inside the US or outside.

References:

- SOX: Europe Balks, US Bends (03/04/05)
  http://www.ecommercetimes.com/story/40905.html?welcome=1203516323
- Europe grabs IPOs as US disclosure rules bite (02/04/06)
  http://www.guardian.co.uk/business/2006/apr/02/theobserver.observerbusiness2
- Europe needs to pull its SOX up (01/29/04)
  http://www.itweek.co.uk/vnunet/news/2124214/europe-needs-pull-sox
- The 8th EU Directive - No SOX for Europe (10/26/07)
  http://www.insidesarbanesoxley.com/2007/11/8th-eu-directive-no-sox-for-europe.asp
- Sarbanes-Oxley Goes Global (07/13/06)
  http://www.forbes.com/2006/07/13/leadership-sarbox-governance-cx_hc_0713sarboxgoesglobal.html

Questions?

Vielen Dank
Bedankt
Merci
Grazie
THANK YOU
Hvala
Gracias

Feedback…

- Your feedback is highly appreciated.
- Use the following information in the evaluation form
  - Speaker Name : Suhas Upadhye
  - Session name :
    - If SOX is for US only, then what's the non-US Oracle DBA got to do with it?
  - Session# : 308
- E-mail : suhasu@niwara.com