

Utilizing Oracle Standard Functionality and other Oracle tools to comply with Sarbanes- Oxley

By
Olga Johnson
City of Detroit

Information on Speaker Olga Johnson

- Title is Business System Support Specialist
- Maintains and teaches the General Ledger and Fixed Assets for the City of Detroit
- Performs setups, writes FSG, test changes, performs upgrades, researches items, and works with other modules that interact with GL and Fixed Assets.

Agenda

- Key Points of Sarbanes Oxley (SOX)
- How to setup responsibilities and limit segments to comply with SOX
- Identity Management, Audit Vault, Database Vault and SOX Compliance
- Release 12 and SOX Compliance

Key points of SOX

- **Sec. 302 Corporate Responsibility for financial reports**
 - Signing officers are responsible for
 - Establishing and maintaining internal controls
 - Ensure material information is prepared periodically
 - Evaluate the effectiveness of internal controls within 90 days of report

Key points of SOX

- **Sec. 302 Corporate Responsibility for financial reports**
 - Signing officers are responsible for
 - Presenting conclusions on effectiveness of internal controls
 - Disclose deficiencies in design or operation of internal controls
 - Disclose fraud whether or not material
 - Indicate significant changes to internal controls

Key points of SOX

- **Sec. 401 Disclosure in periodic reports**
 - Each Financial report should reflect all material correcting adjustments
- **Sec. 404 Management assessment of internal controls**
 - Responsibility for management and establishing and maintaining adequate internal control structure.
 - Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Key points of SOX

- **Criminal Fraud accountability penalties**
 - Destruction, alteration, or falsification of records in federal investigation and bankruptcy... FINE and up to 10 years in prison
 - Failure to certify financial reports... fined up to 1,000,000 and imprisoned up to 10 years
 - Not comport with all requirements set forth... fined not more than 5,000,000 and imprisoned up to 20 years

Example of Internal Controls

- **Segregation of Duties**
 - Responsibilities
 - Limited access to segments

Segregation of Duties-Responsibilities-Matrix

Microsoft Excel - RESPONSIBILITY MATRIX.xls

Book Antiqua 10 B I U 75%

G:\oaug presentation 4-15-08\RESPONSIBILITY MATRIX.xls

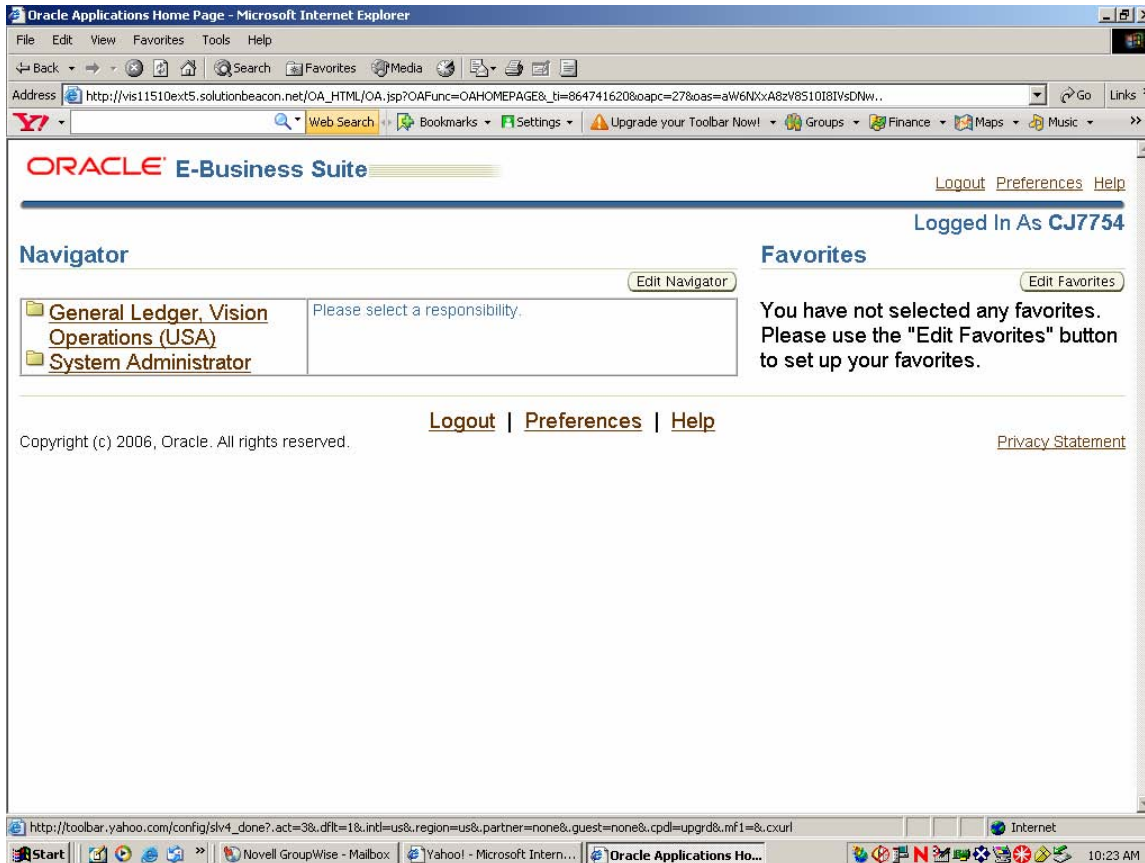
	B	C	D	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	GENERAL LEDGER SUPERUSER			ORAUG GL SUPERUSER																
2	Standard Prompt	Custom Prompt	Description	ORAUG RESOURCE DIVISION																
3				ORAUG SALES DIVISION																
4				ORAUG MANUFACTOR DIVISION																
5				ORAUG POST																
7	Encumbrance		Enter Encumbrance Manual Journals	X	X	X	X													
8	Import			X																
9	Define			X																
10	Generate			X																
11	Schedule			X																
12	AutoAllocation			X																
13	BUDGETS			X																
14	INQUIRY		Perform Inquires	X																
15	Average			X	X	X	X	X												
16	Budget		Inquiry on the Budget	X	X	X	X	X												
17	Journal		Inquiry on Journals	X	X	X	X	X												
18	Account		Inquiry on Accounts	X	X	X	X	X												
19	Account Analysis And Drilldown		Inquiry on Analysis of Accounts and drill to source	X	X	X	X	X												
20	CURRENCY			X																
21	TRANSACTIONS			X																
22	CONSOLIDATION			X																
23	REPORTS			X																
24	SETUP			X																
25	OTHER			X																

OTA Menu

Draw AutoShapes

Start G:\p... Pres... Acce... Micro... SOX... 5:30 PM

Setup Unique Responsibilities



Setup Unique Responsibilities

The screenshot shows the 'Responsibilities' form in Oracle Applications. The form is titled 'Oracle Applications - Solution Beacon Vision 11.5.10.2' and includes a menu bar (File, Edit, View, Folder, Tools, Window, Help) and a toolbar. The main form area is divided into several sections:

- Responsibility Name:** OAUG GL SUPERUSER
- Application:** General Ledger
- Responsibility Key:** OAUG GL SUPERUSER
- Description:** OAUG GL SUPERUSER
- Effective Dates:** From 01-DEC-2007, To (empty)
- Available From:**
 - Oracle Applications
 - Oracle Self Service Web Applications
 - Oracle Mobile Applications
- Data Group:**
 - Name:** Standard
 - Application:** General Ledger
- Request Group:**
 - Name:** GL Concurrent Program Group
 - Application:** General Ledger
- Menu:** GL_SUPERUSER
- Web Host Name:** (empty)
- Web Agent Name:** (empty)

Below these sections are three tabs: 'Menu Exclusions', 'Excluded Items', and 'Securing Attributes'. The 'Menu Exclusions' tab is active, showing a table with columns 'Type', 'Name', and 'Description'. The first row has 'Function' in the 'Type' column. Below the table is a status bar that reads 'FRM-40400: Transaction complete: 1 records applied and saved.' The Windows taskbar at the bottom shows the Start button, several open applications (Novell Gro..., Yahoo!, Oracle Ap..., Create Re..., Oracle Ap..., Oracle A...), and the system clock showing 10:35 AM.

Setup Unique Responsibilities

The screenshot shows the Oracle Applications 'Responsibilities' configuration window. The main form is filled with the following details:

- Responsibility Name:** OAUG RESOURCE DIVISION
- Application:** General Ledger
- Responsibility Key:** GENERAL_LEDGER_OP
- Description:** OAUG RESOURCE DIVISION
- Effective Dates:** From 01-DEC-2007
- Available From:** Oracle Applications (selected)
- Data Group:** Name: Standard, Application: General Ledger
- Request Group:** Name: (empty), Application: (empty)
- Menu:** GL_SUPERUSER
- Web Host Name:** (empty)
- Web Agent Name:** (empty)

A search for 'Post Journals' is performed, resulting in a list of functions:

Name	Description
AutoPost Criteria	Define autopost criteria
Consolidation Workbench: Post	Submit posting on consolidation j
Enter Journals: Post	Post in the Enter Journals or Enter
Post Journals	Post journals
Run AutoPost Requests	Run autopost requests

The 'Post Journals' function is highlighted in the list. The window also shows 'Menu Exclusions' and 'Securing Attributes' tabs, and a status bar at the bottom indicating 'Choices in list: 396'.

Setup Unique Posting Responsibility

The screenshot shows the 'Menus' window in Oracle Applications. The menu configuration is as follows:

- Menu: **OAUG_POST**
- User Menu Name: **General Ledger Posting**
- Menu Type: **Standard**
- Description: **GL POST**

Seq	Prompt	Submenu	Function	Description	Grant
1	Auto post	GL_SUPERUSER	AutoPost Criteria	Ability to Auto Post	<input checked="" type="checkbox"/>
2	Post Journal	GL_SUPERUSER	Post Journals	Ability to post journals	<input checked="" type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>

Setup Unique Posting Responsibility

The screenshot shows the 'Responsibilities' form in Oracle Applications. The form is titled 'Responsibilities' and contains the following fields and sections:

- Responsibility Name:** OAUG POST
- Application:** General Ledger
- Responsibility Key:** OAUG POST
- Description:** (empty)
- Effective Dates:** From 20-FEB-2008, To (empty)
- Available From:**
 - Oracle Applications
 - Oracle Self Service Web Applications
 - Oracle Mobile Applications
- Data Group:**
 - Name:** Standard
 - Application:** General Ledger
- Menu:** General Ledger Posting
- Web Host Name:** (empty)
- Web Agent Name:** (empty)
- Request Group:**
 - Name:** (empty)
 - Application:** (empty)
- Menu Exclusions:** Excluded Items, Securing Attributes
- Table:**

Type	Name	Description
Function		

At the bottom of the form, a status bar reads: FRM-40400: Transaction complete: 1 records applied and saved.

Assigning Responsibility to an User

The screenshot shows the Oracle Applications 'Users' form. The user name is 'MR.SOX POST', description is 'OAUG AND SOX', and password expiration is set to 5 days. The 'Direct Responsibilities' tab is active, showing a table with one entry: 'OAUG POST' responsibility for the 'General Ledger' application, with a 'Standard' security group and an effective date starting on '20-FEB-2008'.

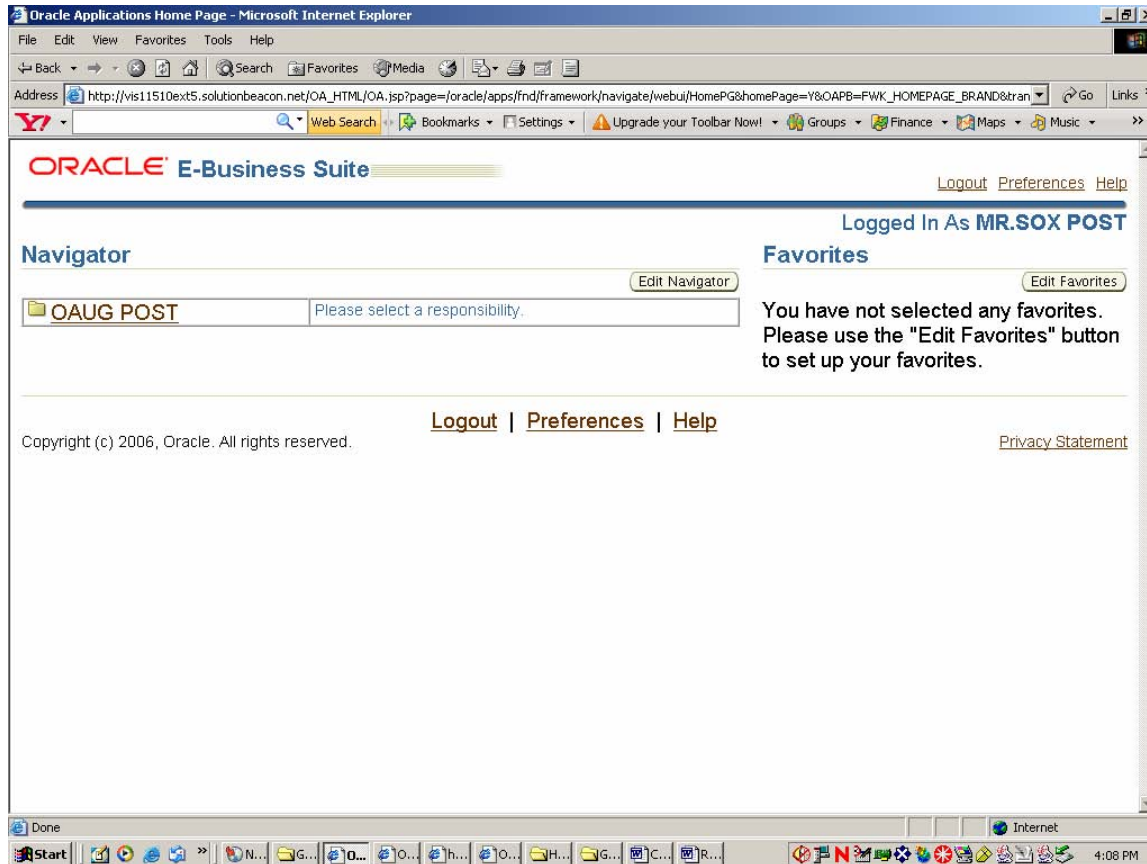
User Information:

- User Name: MR.SOX POST
- Password: [Empty]
- Description: OAUG AND SOX
- Person: [Empty]
- Customer: [Empty]
- Supplier: [Empty]
- E-Mail: [Empty]
- Fax: [Empty]
- Effective Dates: From 20-FEB-2008, To [Empty]
- Password Expiration: Days 5

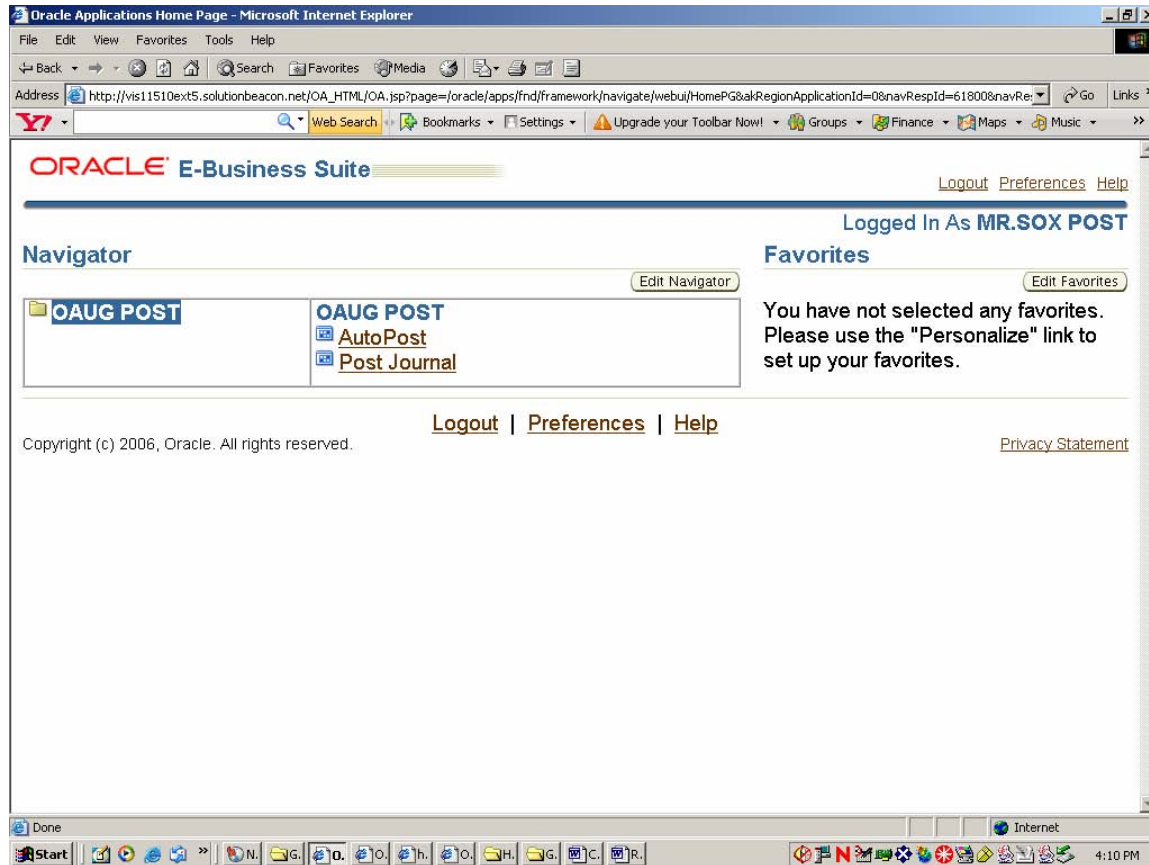
Direct Responsibilities Table:

Responsibility	Application	Description	Security Group	From	To
OAUG POST	General Ledger		Standard	20-FEB-2008	

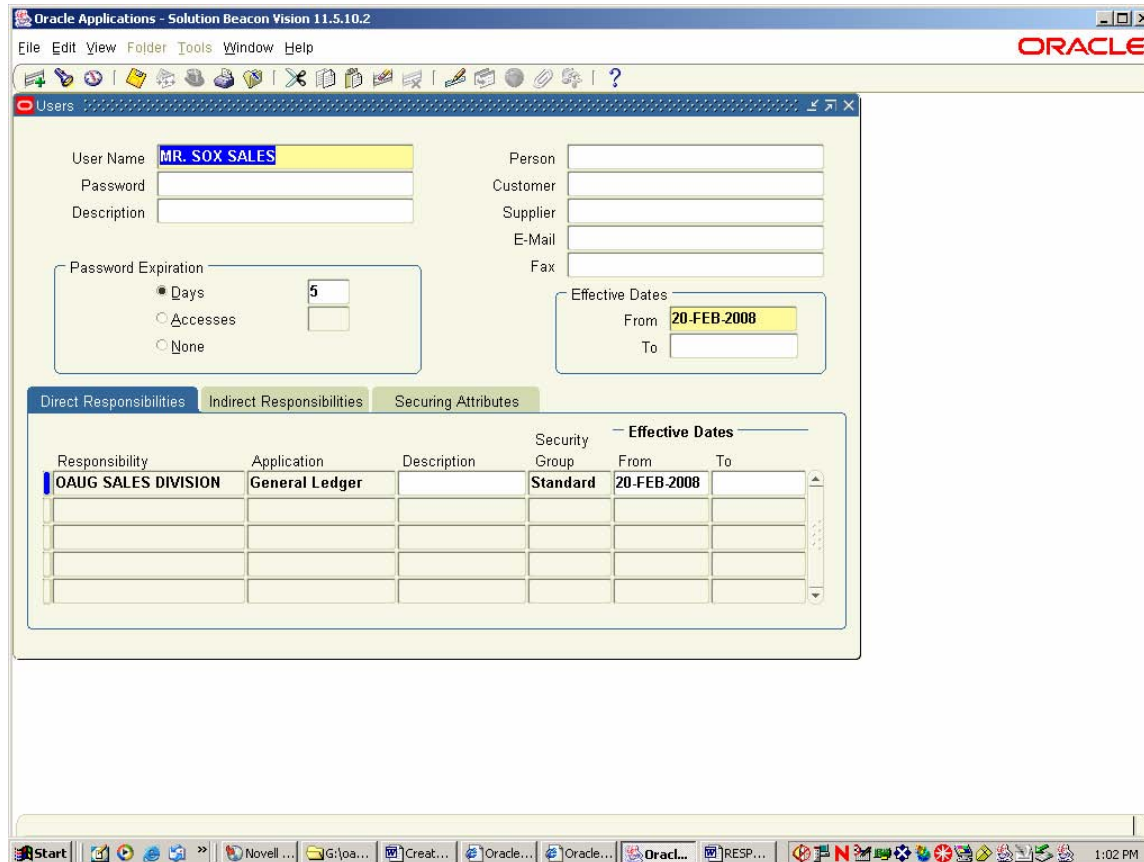
Assigning a Responsibility to an User



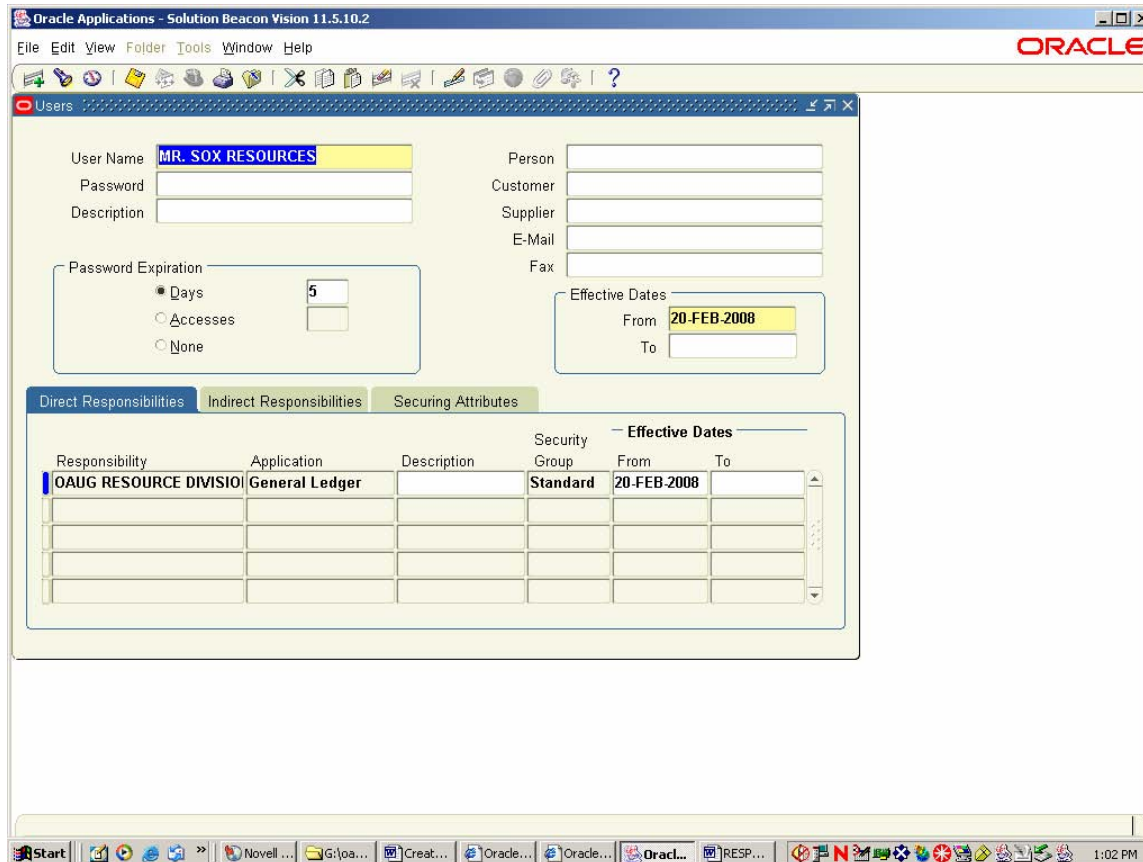
Assigning a Responsibility to an User



Assigning a Responsibility to an User



Assigning a Responsibility to an User

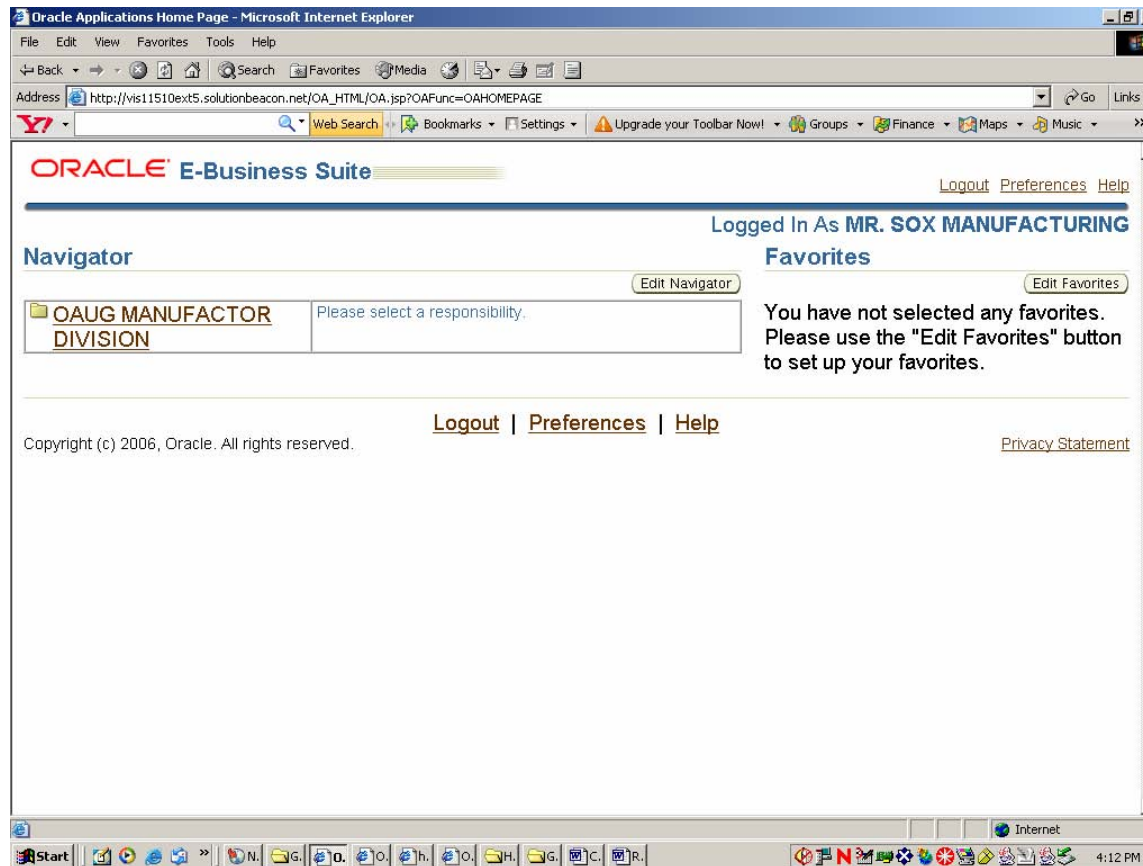


Assigning a Responsibility to an User

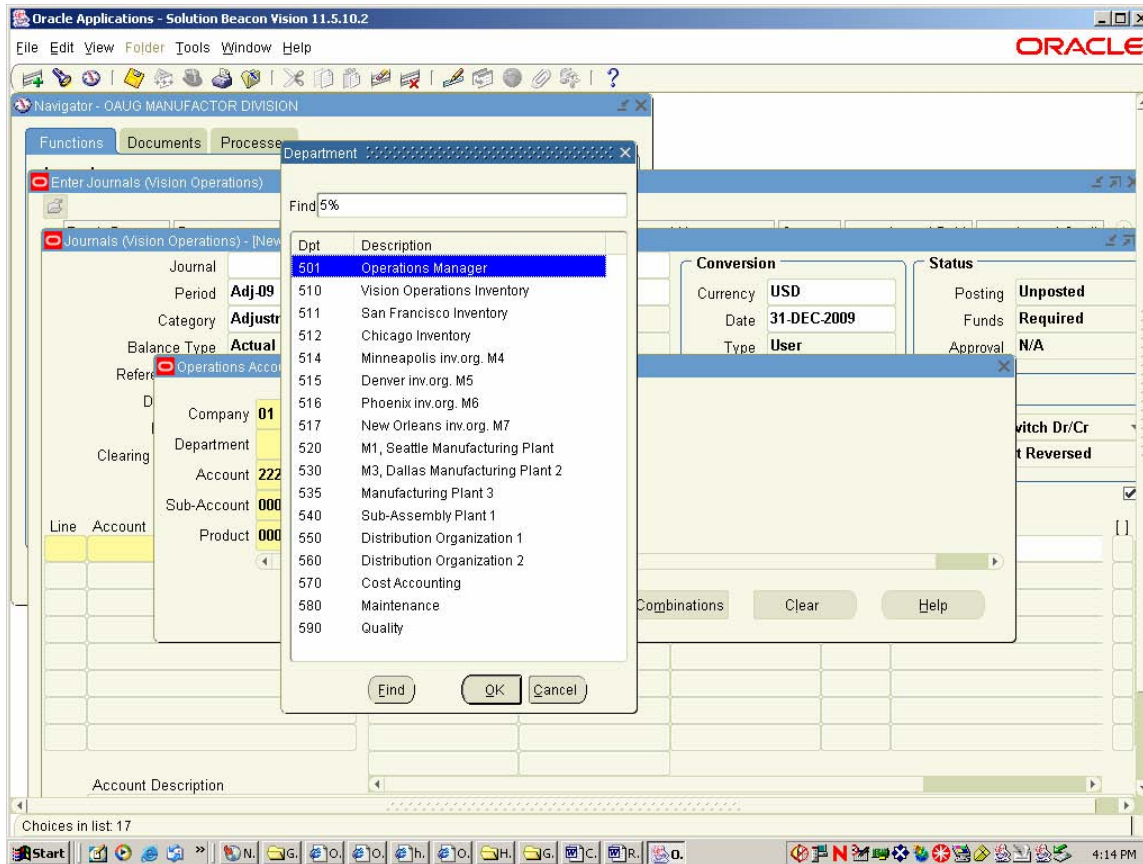
The screenshot shows the Oracle Applications 'Users' form. The 'User Name' field is populated with 'MR. SOX MANUFACTURING'. The 'Effective Dates' section shows 'From' as '20-FEB-2008'. Below, the 'Direct Responsibilities' tab is active, displaying a table with the following data:

Responsibility	Application	Description	Security Group	From	To
OAUG MANUFACTOR DIVIS	General Ledger	MANUFACTORINC	Standard	20-FEB-2008	

Assigning a Responsibility to an User



Assigning a Responsibility to an User



Separation by department

3 Major Department Division
Each Department should only see their department accounts

Translated Value	Description	Translated Value	Description	Translated Description
100	Resources	400	Sales	500 Manufacturing
110	Facilities Resources	401	Regional Sales Management	501 Operations Manager
111	West Region Resources	402	CEO, Kurt Elkins	510 Vision Operations Inventory
112	East Region Resources	404	Consulting Sales	511 San Francisco Inventory
120	Machine Resources	410	International Sales	512 Chicago Inventory
130	Computer Resources	420	Sales East	514 Minneapolis inv.org. M4
140	Communications Resources	421	Sales NorthEast	515 Denver inv.org. M5
		422	Sales Mid-Atlantic	516 Phoenix inv.org. M6
		423	Sales SouthEast	517 New Orleans inv.org. M7
		430	Sales South	520 M1, Seattle Manufacturing Plant
		440	Sales Central	530 M3, Dallas Manufacturing Plant 2
		450	Sales West	535 Manufacturing Plant 3
		460	Government Sales	540 Sub-Assembly Plant 1
		470	Education Sales	550 Distribution Organization 1
		471	Education Sales 2	560 Distribution Organization 2
		480	Service Contracts	570 Cost Accounting
		490	Marketing	580 Maintenance
				590 Quality

Separation by Department

The screenshot shows the 'Define Security Rules' window in Oracle Applications. The 'Value Set' is named 'department'. The 'Security Rules' table is as follows:

Name	Description	Message
OAUG Resource	OAUG Resource Division	OAUG Resource Division100-199
OAUG Sales	OAUG Sales Division	OAUG Sales Division 400-499
OAUG Manufa	OAUG Manufacturing	OAUG Manufacturing 500-599

The 'Security Rule Elements' table is as follows:

Type	From	To
Include	0000	9999
Exclude	0000	0099
Exclude	0200	9999

An 'Assign' button is located at the bottom right of the window.

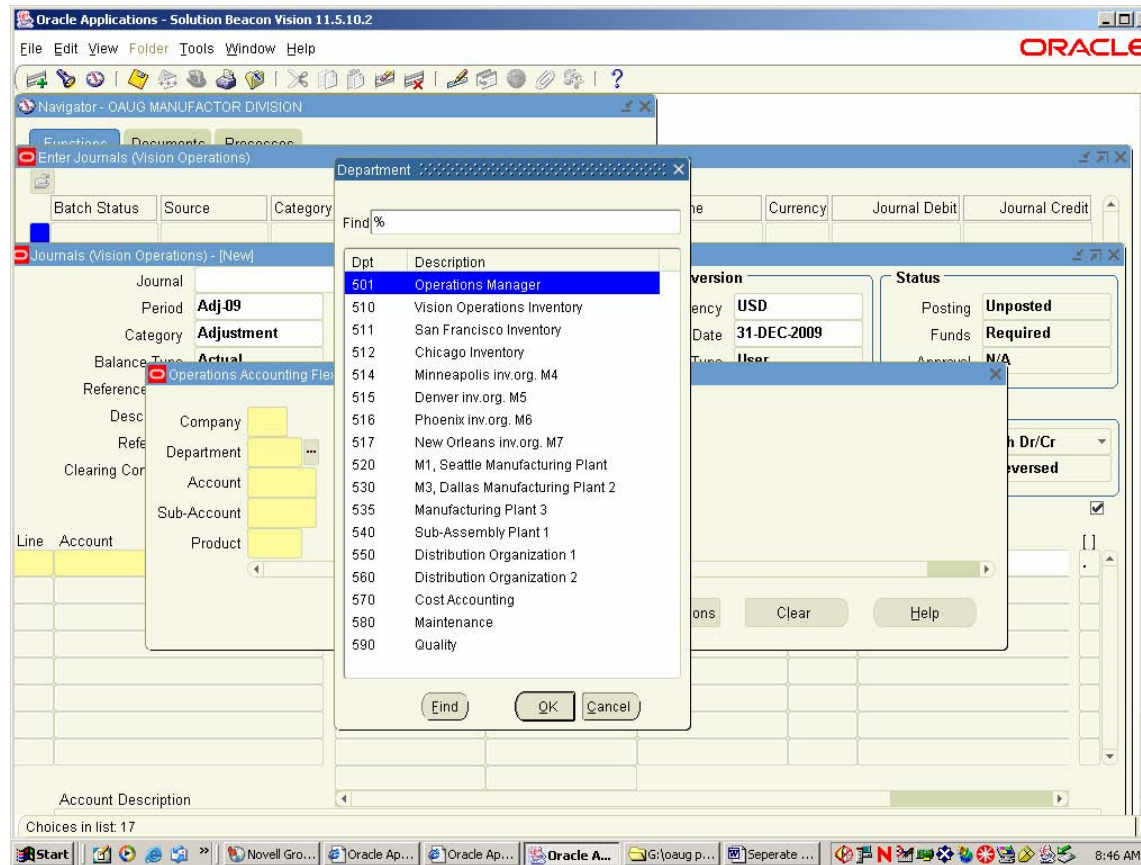
Separation by Department

The screenshot shows the 'Assign Security Rules' window in Oracle Applications. The 'Value Set' tab is selected, with the name 'department' entered. Below this, there are fields for 'Dependent Value Set' and 'Independent Value Set'. The 'Security Rules' section contains a table with the following data:

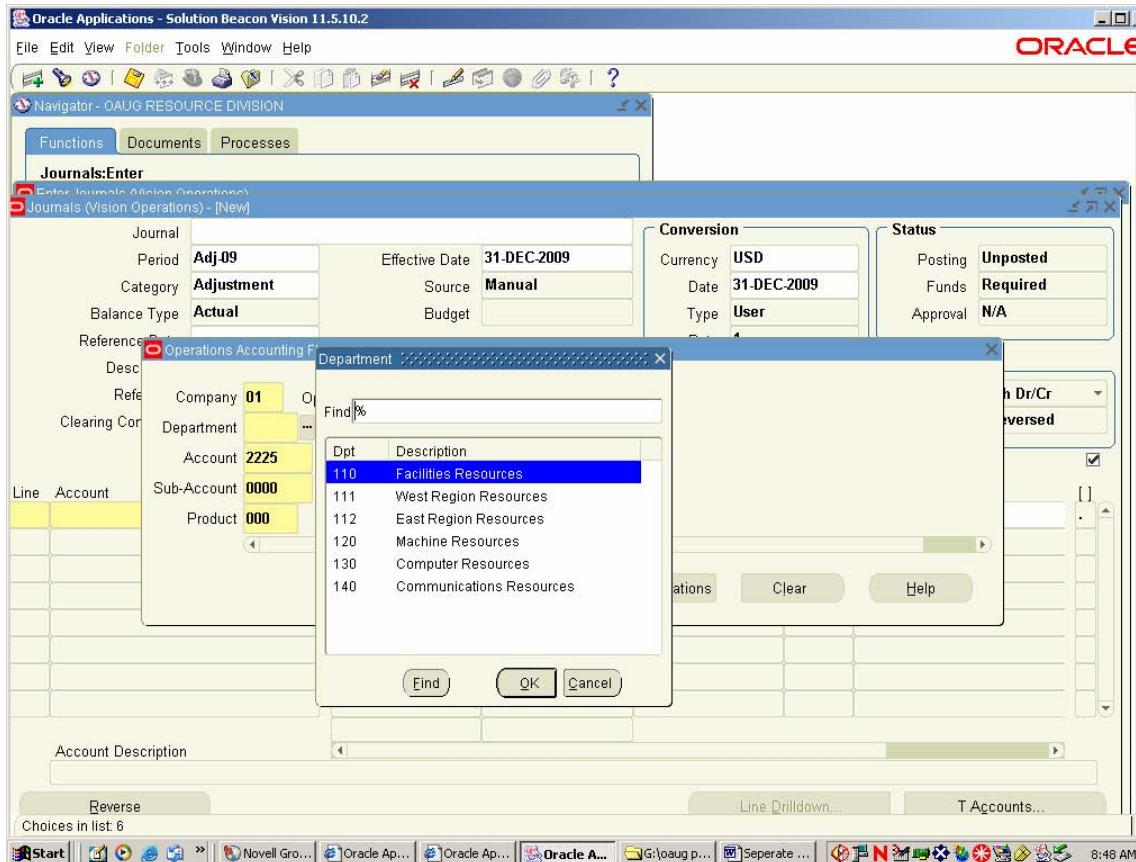
Application	Responsibility	Name
General Ledger	OAUG RESOURCE DIVISION	OAUG Resource
General Ledger	OAUG SALES DIVISION	OAUG Sales
General Ledger	OAUG MANUFACTOR DIVISION	OAUG Manufacturer

Below the table, the 'Description' is 'OAUG Resource Division' and the 'Message' is 'OAUG Resource Division100-199'. An 'Assign' button is located at the bottom right of the window.

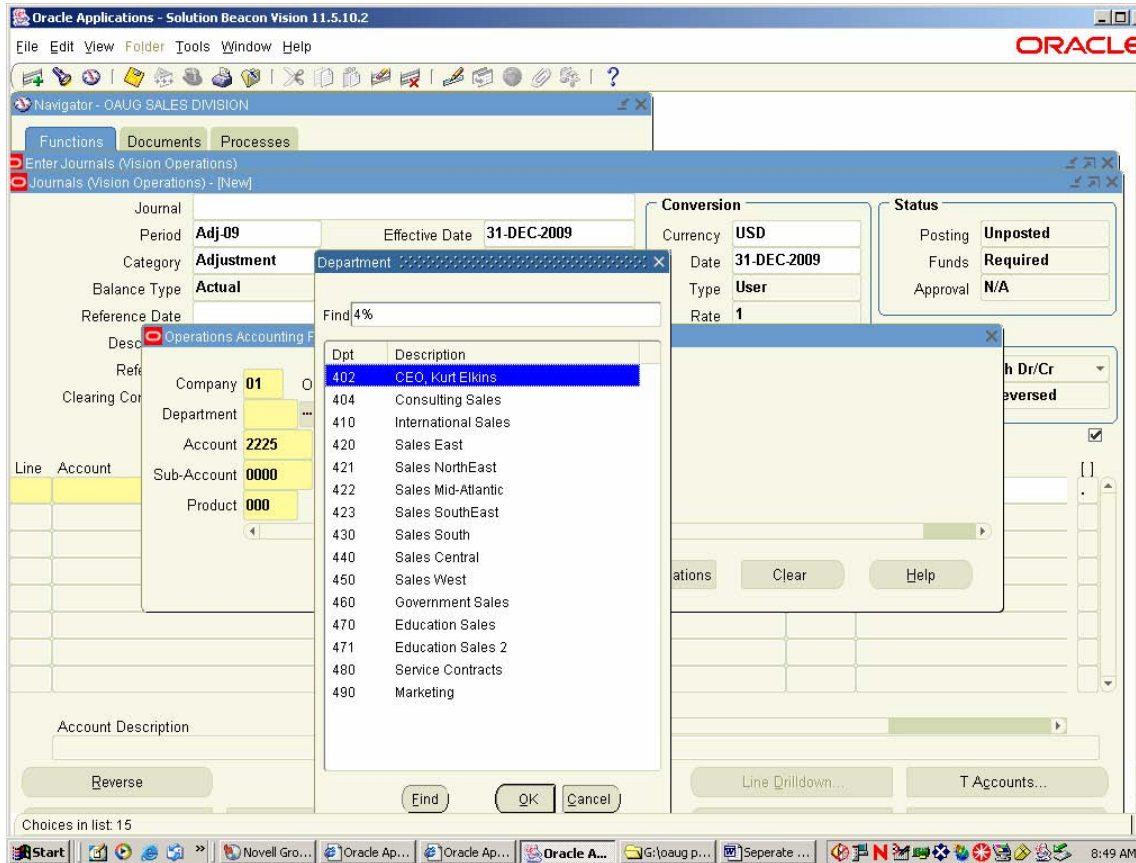
Separation by Department



Separation by Department



Separation by Department



Identity Management

- Financial Compliance
 - SOX (Sarbanes-Oxley or SarbOx)
 - Michigan Senate Bill- 309
 - Other current and future regulations

Sox and Identity Management Components

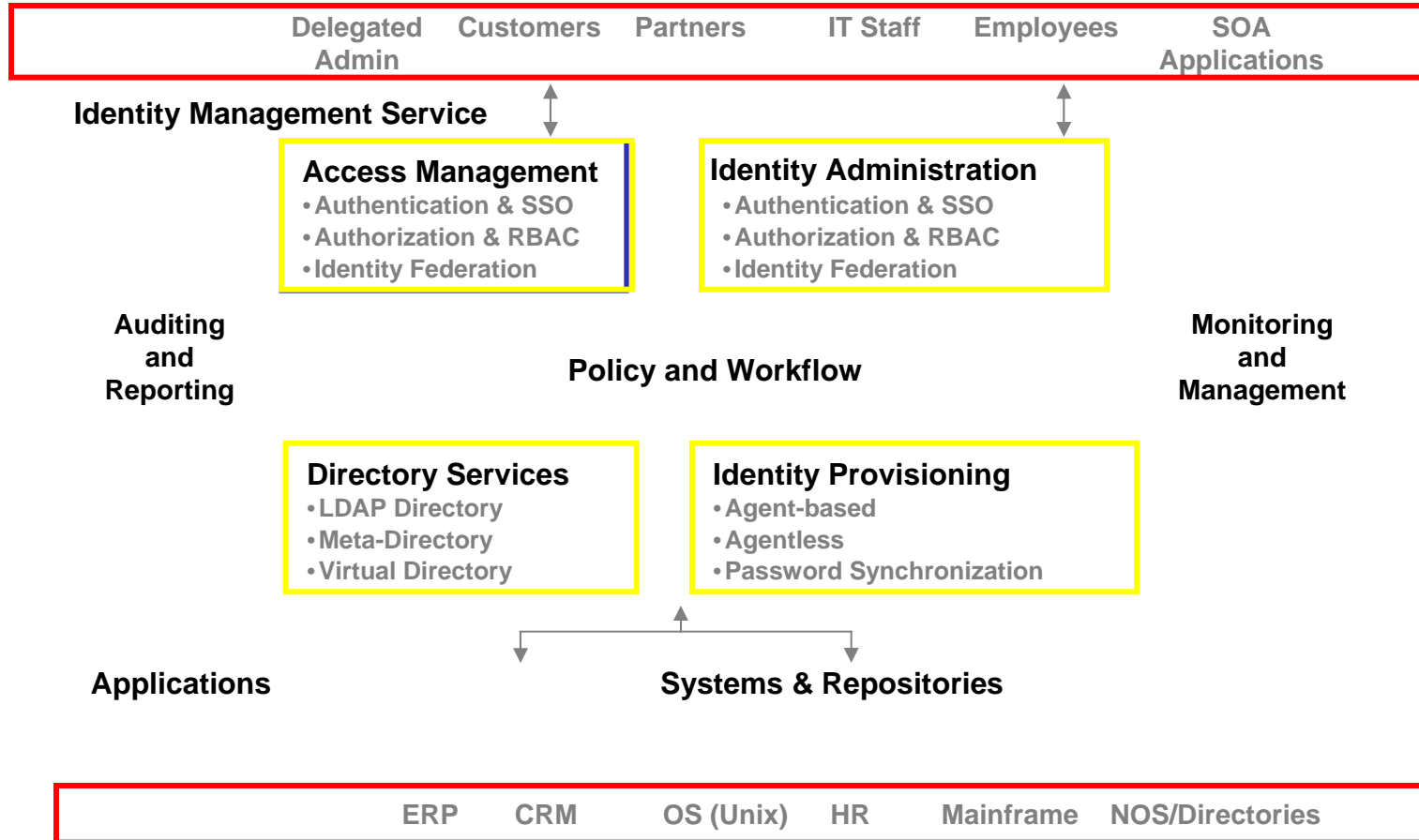
- Oracle Identity Federation
- Oracle Web Access Manager
- Oracle Web Service Manager
- Oracle Enterprise Single Sign-on

Sox and Identity Management Components

- Oracle Identity Manager
- Oracle Access Manager
- Oracle Virtual Directory
- Oracle Internet Directory

Enterprise Identity Management

External Internal



Oracle Identity Federation

- **Features**
 - Identity and trust sharing across business partners, both as Service Provider (Hub) or Identity Provider (Spoke)
 - Lightweight, multi-protocol gateway – SAML, Liberty, WS-Federation
 - Integrates with leading Identity Management platforms



Oracle Identity Federation

- **Benefits**
 - Reduced cost of interaction between business partners
 - Reduce administration cost
 - Deliver improved end user experience



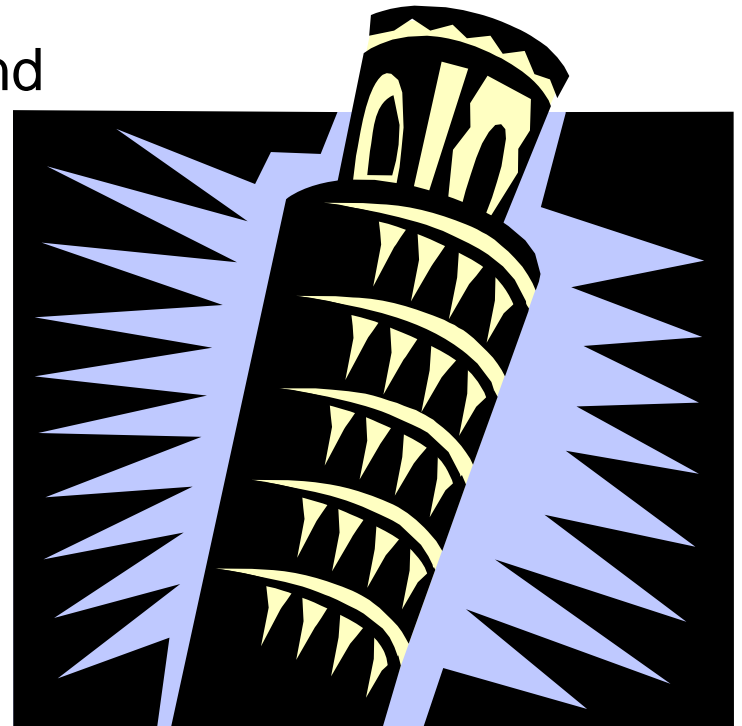
Oracle Identity Federation

- **Differentiators**
 - Self-contained, easy to deploy solution
 - Flexible deployment configurations
 - Rich, 100% web-based configuration interfaces for improved administrator and end user experience
 - Proven scalability - large production deployments



Oracle Internet Directory

- **Features**
 - Full feature LDAP server with a RDBMS data-store
 - Industry leading scalability and HA capabilities
 - Strong Oracle Platform integration
 - VSLDAP certified and EAL4 compliant



Oracle Internet Directory

- **Benefits**
 - Reduced operational cost with Oracle Grid support
 - Seamless integration with Oracle Applications and Products



Oracle Internet Directory

- **Differentiators**
 - RDBMS backend provides proven scalability & performance
 - Rich, built in auditing of all events and operations
 - Flexible data replication and redundancy features
 - Ships with built-in directory integration functionality



Oracle Virtual Directory

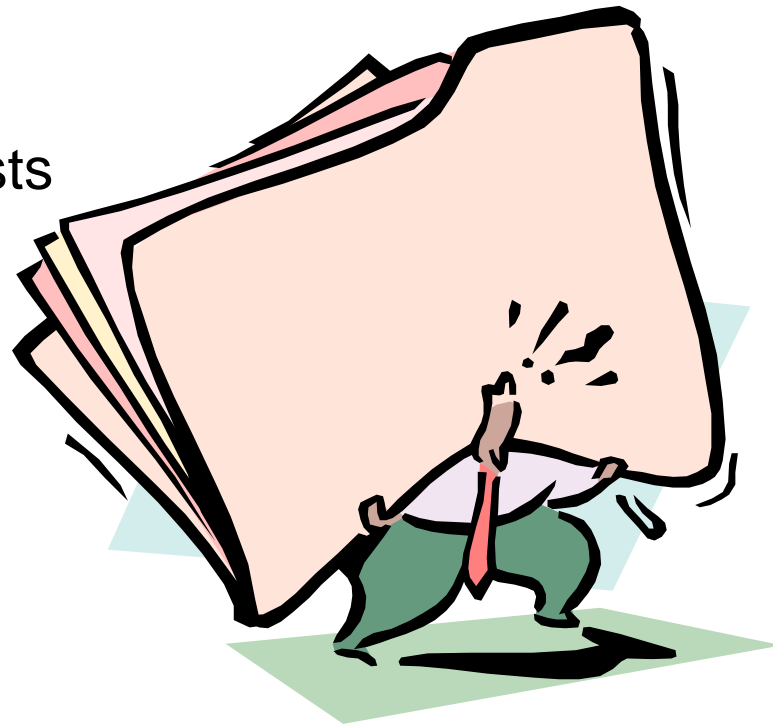
- **Features**

- Virtualization, Proxy, Join & Routing capabilities
- Modern Java & Web Services technology
- Superior extensibility
- Scalable multi-site administration
- Direct data access



Oracle Virtual Directory

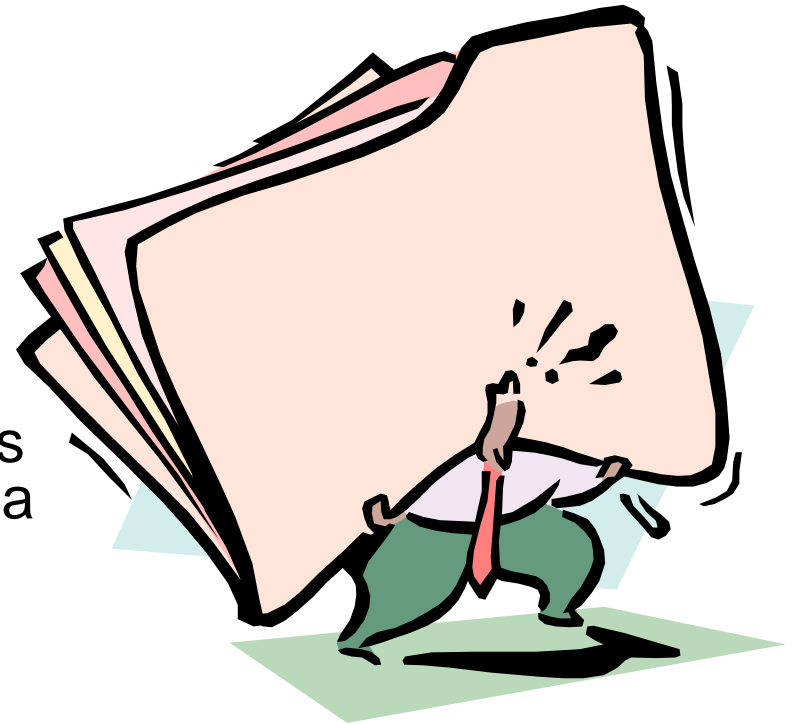
- **Benefits**
 - Perform Real-time directory integration
 - Accelerate application deployment
 - Lower development costs



Oracle Virtual Directory

- **Differentiators**

- Lightweight & flexible architecture
- Supports true virtualization without local cache, enabling stringent policy or privacy requirements
- Modular architecture supports the addition of connectors to a wide array of identity stores



Oracle Access Manager

- **Features**

- Multi-level, multi-factor authentication
- Web and App server level authorization
- Workflow driven Self-service & Delegated administration
- Services-based architecture eases integration with existing IT infrastructure



Oracle Access Manager

- **Benefits**
 - Policy-based access management
 - Centralized and consistent security across heterogeneous environments
 - Reduced administration cost
 - Increased IT governance and compliance readiness



Oracle Access Manager

- **Differentiators**
 - Administrative scalability via workflow and delegation
 - Access control leverages up to date identity information
 - Comprehensive auditing to a common database



Database Vault, Audit Vault and SOX

Audit Vault

Protect data with AV Security by the Administrator



Report on data with Alerts and Reports

Store data with AV Archiver and AV Audit Collection

Audit Vault Alert Report Sample from Oracle

ORACLE Enterprise Manager 10g
Audit Vault

[Help](#) [Logout](#)

Audit Report Management

Dashboard | Event Report | **Alert Report**

Database Instance: avdb > Alert Report

Alert Report

Alert:

Alert Severity: ALL

Source:

User:

Event Category:

Event:

Object:

Event Time: Last 24 Hours Last One Week Last One Month

Calendar From To

Select	Alert	Alert Severity	Source	User	Event Category	Event	Object	Event Time
<input checked="" type="radio"/>	OE_PRODUCT_INFO	CRITICAL	123.23.5.34	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:32:49
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	123.23.5.34	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:32:49
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	OE_DB.US.ORACLE.COM	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:21:04
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	123.23.5.34	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:21:04
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	123.23.5.34	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:20:26
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	OE_DB.US.ORACLE.COM	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:20:25
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	OE_DB.US.ORACLE.COM	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:07:56
<input type="radio"/>	OE_PRODUCT_INFO	CRITICAL	OE_DB.US.ORACLE.COM	SYS	DATA ACCESS	UPDATE	PRODUCT_INFORMATION	06/05/2006 23:07:56

Audit Vault Dashboard Sample from Oracle

ORACLE Enterprise Manager 10g
Audit Vault

Help Logout
Audit Report Management

Dashboard | Event Report | Alert Report

Database Instance: avdb

Dashboard

* From * To

Overall Alert Severity

Showing alert distribution by severity across all sources

Severity	Count
Severity 1 (WARNING)	6
Severity 2 (CRITICAL)	23
Severity 3 (INFO)	9

Overall Alert Activity

Showing alert distribution by source

Source Type	Count
Affected Sources	2
Unaffected Sources	4

Affected Sources : Sources with alerts raised

Sources with High Alert Activity

Showing sources with highest amount of alerts

Source	Severity 1	Severity 2	Severity 3
OE_DB.US.ORACLE.COM	1	10	2
123.23.5.34	2	15	3

Alerts by Audit Event Category

Showing amount of alerts by audit event category

Audit Event Category	Number Of Alerts
System Management	0
Account Management	1
Object Management	1
Application Management	2
Role And Privilege Management	0
Data Access	32
User Session	1
Peer Association	0
Service And Application Utilization	0
Exceptional	0
Audit	1
Unknown	0

Activities

Showing activities by audit event category

Database Vault

- Prevent DBA from seeing Medical information, Social Security numbers and other regulated data.
- Enforce data access through the application?
- Prevent un-authorized modifications to the application and database?

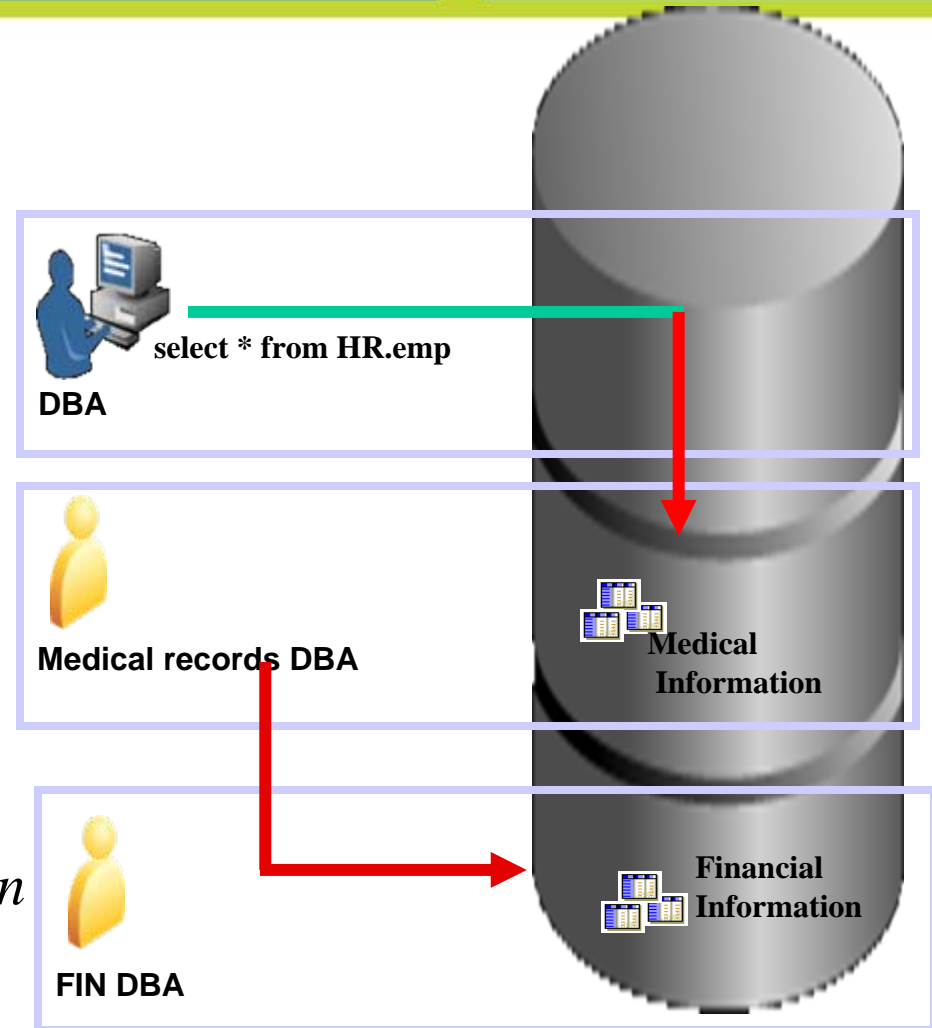
Oracle Database Vault Realms

- **Database DBA attempts to views Medical data**

Insider access to data can be controlled

- **Medical Records DBA attempts to views Fin. data**

Security risk from server consolidation can be controlled with realms.



Realms can be easily applied to existing applications with minimal performance impact

Database Vault administration view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)

[Database](#)

Logged in as DBV_OWNER

Database Instance: orcl

[Administration](#) [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Database Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Database Vault Feature Administration

[Realms](#)

[Command Rules](#)

[Factors](#)

[Rule Sets](#)

[Secure Application Roles](#)

[Label Security Integration](#)

[Administration](#) [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

[Database](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2006, Oracle. All rights reserved.
[About Oracle Database Vault Administrator](#)

Database Vault view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Realms

Logged in as DBV_OWNER


Realms

Database Vault realms provide a capability to classify database schemas and database roles into functional groups in order to provide fine-grained access control of the ability to use system level privileges against these types of database objects.

Create

Edit

Remove

Select	Name 	Audit Options	Oracle Defined Realm?	Objects Protected?	Users Authorized?	Status
<input checked="" type="radio"/>	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓

Edit

Remove

Database | [Help](#) | [Logout](#)

Database Vault view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)
Database

Database Instance: [orcl](#) > [Realm](#) > Create Realm

Logged in as DBV_OWNER

Create Realm

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

[Database](#) | [Help](#) | [Logout](#)

Database Vault view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > [Realms](#) > [Edit Realm: HR Realm](#) > Create Realm Secured Object

Logged in as DBV_OWNER

Create Realm Secured Object

Cancel OK

Define a database schema or database role that is protected by the realm.

Object Owner

HR

Object Type

%

Object Name

%

Cancel OK

Database | [Help](#) | [Logout](#)

Database Vault view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Realms

Logged in as DBV_OWNER


Realms

Database Vault realms provide a capability to classify database schemas and database roles into functional groups in order to provide fine-grained access control of the ability to use system level privileges against these types of database objects.

Create

Edit

Remove

Select	Name 	Audit Options	Oracle Defined Realm?	Objects Protected?	Users Authorized?	Status
<input checked="" type="radio"/>	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	HR Realm	Audit On Failure		✓	✗	✓
<input type="radio"/>	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓

Edit

Remove

Database | [Help](#) | [Logout](#)

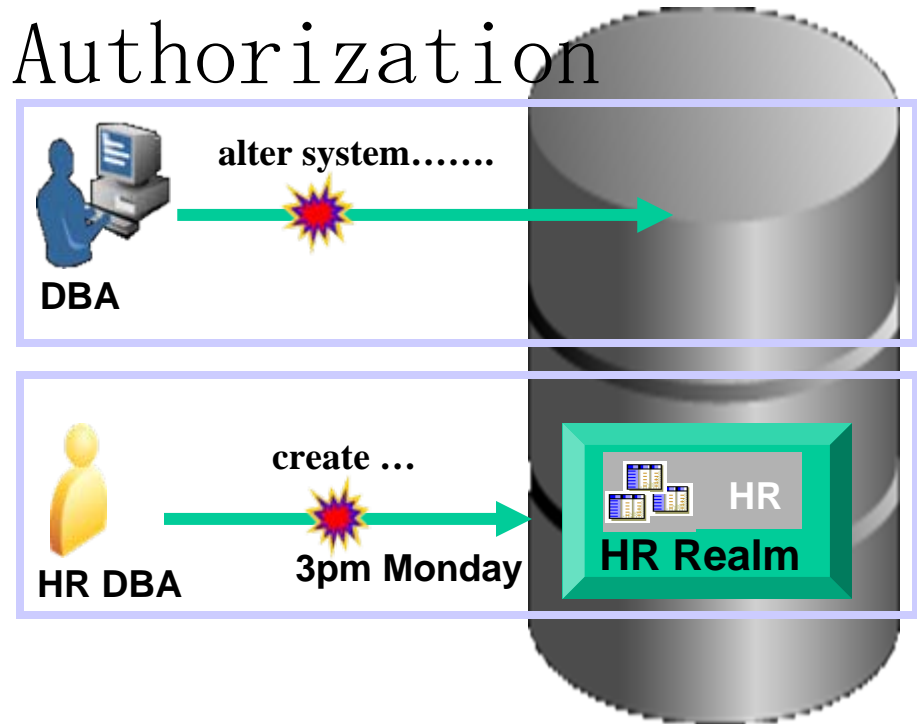
Oracle Database Vault Rules & Multi-factor Authorization

- **Database DBA attempts remote to make changes**

*Rule based on IP
Address blocks action*

- **HR DBA performs unauthorized actions during production**

*Rule based on Date and
Time blocks action*



Slide by Oracle

Factors and Command Rules provide flexible and adaptable security controls

Database Vault view supplied by Oracle

ORACLE Database Vault

[Help](#) [Logout](#)
Database

Database Instance: orcl > Command Rules


Logged in as DBV_OWNER

Command Rules

Command rules control the ability to process Data Definition Language (DDL) commands and special database operations. Command rules determine whether or not to allow the command to succeed based on the evaluation of a Database Vault rule set.

Create

Edit Remove

Select	Command 	Object Owner	Object Name	Rule Set Name	Status
<input checked="" type="radio"/>	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	ALTER USER	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	CREATE USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	GRANT	SYS	DBMS_RLS	Can Grant VPD Administration	✓
<input type="radio"/>	REVOKE	SYS	DBMS_RLS	Can Grant VPD Administration	✓

Edit Remove

Database | [Help](#) | [Logout](#)

Built-In Factors

-Authentication Method

-Domain

-Session User

-Database Name

-Database Instance

-Database IP

-Database Hostname

-Database Instance

-Time

-Enterprise Identity

-Date

-Machine Name

-Machine

-Enterprise Identity

-Language

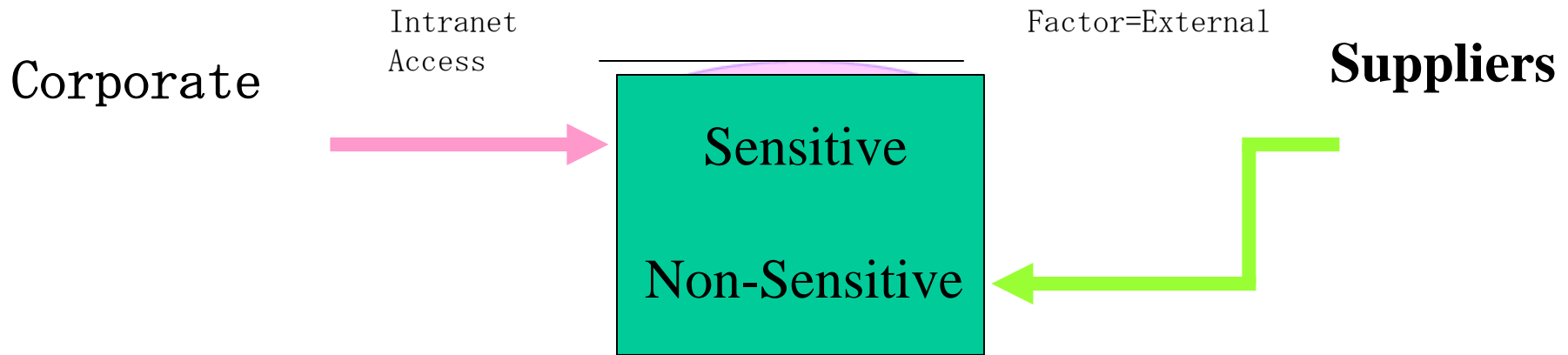
-Network Protocol

-Date

* Additional factors can be defined

Oracle Supplied Slide

Oracle Label Security Integration



Oracle Label Security Restricts Access To Labeled Data Based On Database Vault Factors

SOX and R12 General Ledger

- Profile Option
 - SLA: Enable Sub ledger Transaction Security in GL This enforces the transaction security of the application owning the transaction
 - When data is sent to GL from payables you have three options Draft...Final...Final Post

Conclusion

- Internal Controls-Segregation of Duties
- Internal Controls-Identity Management
- Reporting on and managing Internal controls
Audit Vault and Database Vault
- Release 12 and SOX

THANK YOU!

A SPECIAL THANKS TO:

Norman White
Audrey Jackson
Solution Beacon
Oracle

SOX and Oracle

- Questions and Answers
- Email address:
Johnson@acct.ci.detroit.mi.us