Utilizing Oracle standard functionality and other tools to comply with Sarbanes-Oxley

Olga Johnson
City of Detroit

Introduction:

With over forty agencies and nearly 18,000 employees, the City of Detroit, Michigan operates on a 3.3 billion-dollar annual budget. To ensure that every dollar is accounted for and all expenditures are properly reported, City officials initiated the Detroit Resource Management System (DRMS). Using Oracle software as its base, DRMS has been in service since April 1999. Since then the system has been upgraded several times. The City is now running Oracle Financial 11.5.10.2 and intends to remain current with future releases. Today we are utilizing the General Ledger, Capital Assets, Grants and Projects, Accounts Payable, Purchasing and Receivables Modules. We are implementing Treasury, Cash Management, and Payroll and Human Resource modules. Oracle Training Administration (OTA) serves as the City's official record of employee training.

We are investigating and enhancing our internal controls in a proactive manner. As a result the information presented in this paper was collected as possible solutions. Investigating the requirements of Sarbanes-Oxley (Including Auditing Standards 5) gives us a proactive stance on future regulation such as Senate Bill 309 in Michigan.

A Review of Sarbanes-Oxley:

SOX is known as the Public company Accounting reform and Investor Protection Act of 2002. The Act is named after Senator Paul Sarbanes and Representative Michael G. Oxley. SOX apply to U.S. public companies boards, management and public accounting firms. The Public company Accounting Oversight Board (PCAOB) oversees, regulates, disciplines and inspects accounting firms. Auditors must be independent of the companies they are auditing.

Sec. 302 Corporate Responsibility for financial reports is summarized as follows:

Signing officer must review the Financial Reports

The report should not contain any untrue statements of a material fact or omit to state a material fact, in essence statements should not be misleading

Signing Officers must maintain internal controls; evaluate the internal controls 90 days prior to the report.

Signing Officers must present conclusions about the financial statement report.

The signing must ensure the internal controls lead to a statement, which includes all material information relating to the entity, and it consolidated subsidiaries.

The signing Officers must disclose to the Board of directors and Auditors all significant deficiencies and material weakness in internal controls. Any fraud material or not should be disclosed. Corrective actions to internal controls should be disclosed. The proper utilization of an Oracle ERP system can greatly help Management meet the goals of applying internal controls and report on them in a timely manner. In this paper we deal mainly with the internal control of separation of duties and reporting on these controls.

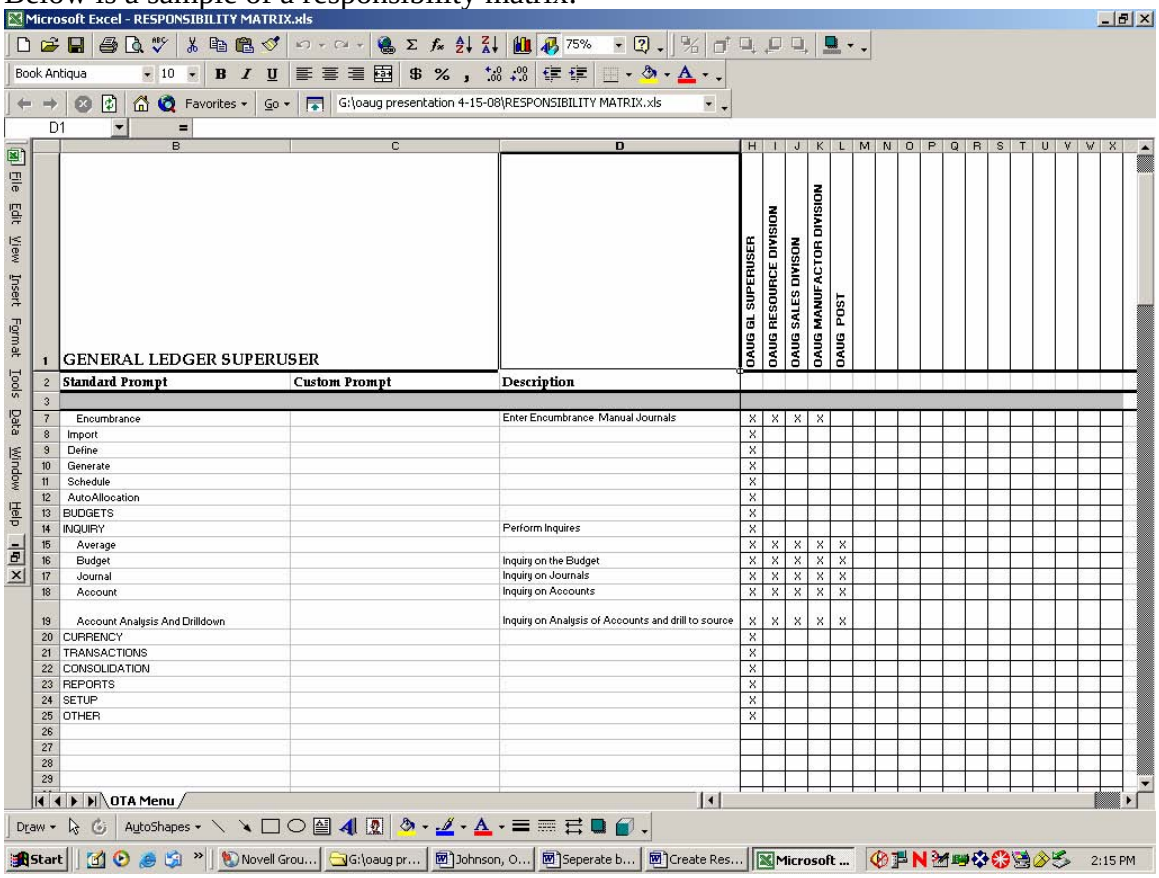
SOX deal with Information technology and controls that relate to the accuracy of financial reports. This presentation addresses controls that can be implemented to ensure the correctness of financial statements and reduce the occurrence of fraud as related to Information Technology functionality. SOX have stiff penalties for non-compliance and attempt to hide non-compliance. The penalty can be a maximum of 10-20 years in prison and 1,000,000-5,000,000 in fines. The penalty depends on the violation and handling of the violation. A major way to comply with SOX is to limit what can be seen, changed, entered into a system and to report on this activity. In this paper will address segregation of duties, reporting on internal control and access to the IT systems related to financial data. Some of the tools provided to comply with SOX will also meet compliance standards for other laws such as HIPPA and Michigan Senate Bill 309.

COPYRIGHT @ 2008 BY Olga Johnson

Responsibility Segregation:

Oracle standard functionality lets you create responsibilities and allow the end-users to access menu items that want them to have rights to perform specific duties. This is setup utilizing the System Administrator Responsibility. Several seeded responsibilities are already available in Oracle. A suggest way to begin is to copy the super user responsibility and give it an acronym at the beginning that denotes it is unique to your system. In this paper we are utilizing OAUG as the acronym. The first step is to determine what responsibilities you want to create and what you menu items they should have rights to utilize.

Below is a sample of a responsibility matrix:

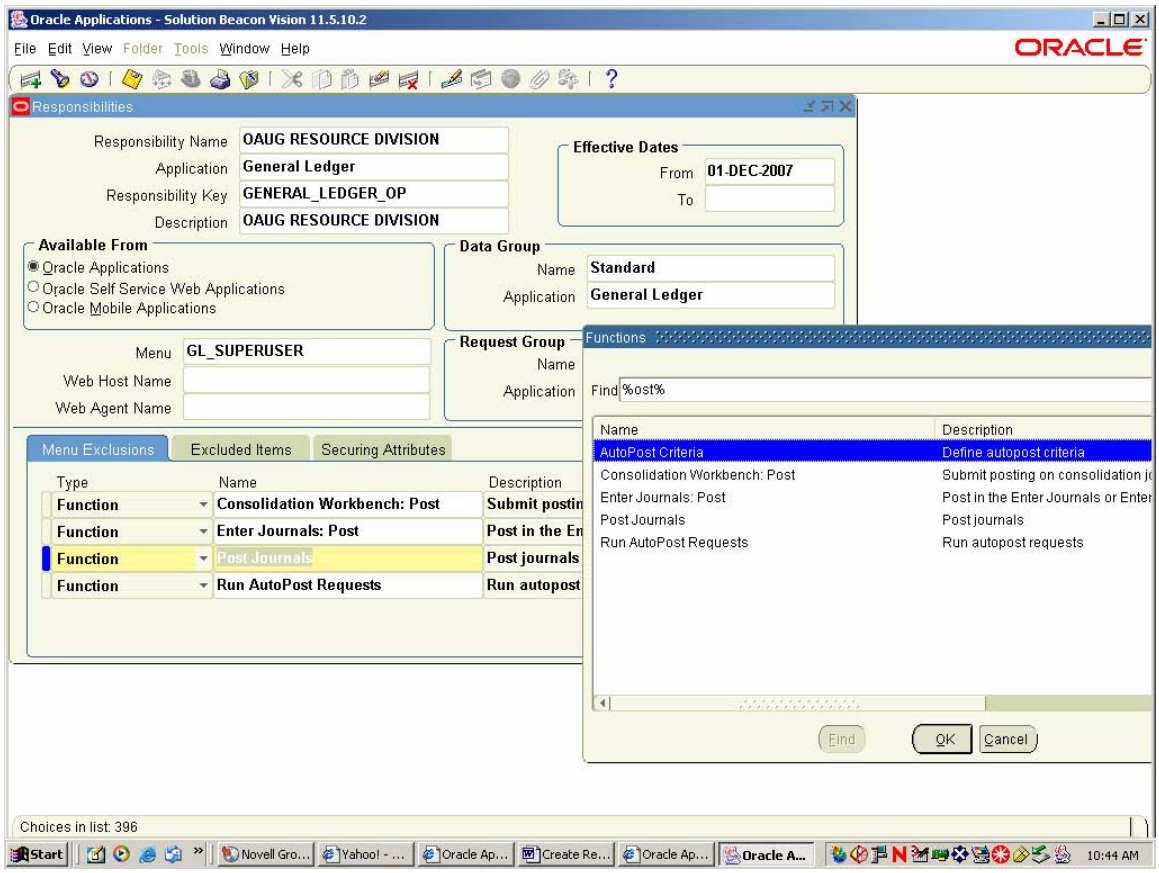


	B	C	D	H	I	J	K	L
1	GENERAL LEDGER SUPERUSER			OAUG GL SUPERUSER	OAUG RESOURCE DIVISION	OAUG SALES DIVISON	OAUG MANUFACTOR DIVISION	OAUG POST
2	**Standard Prompt**	**Custom Prompt**	**Description**					
3								
7	Encumbrance		Enter Encumbrance Manual Journals	X	X	X	X	
8	Import			X				
9	Define			X				
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				
26								
27								
28								
29								

A brief description of the responsibility matrix:

The standard prompt is taken from the menu item of the Super user responsibility you want to segregate. The top of the form shows the various responsibilities and the x's in the columns denote what menu item to give each responsibility. The next step is to sign on the Oracles System Administrator responsibility. Navigate ->Security->responsibility->Define.

COPYRIGHT @ 2008 BY Olga Johnson



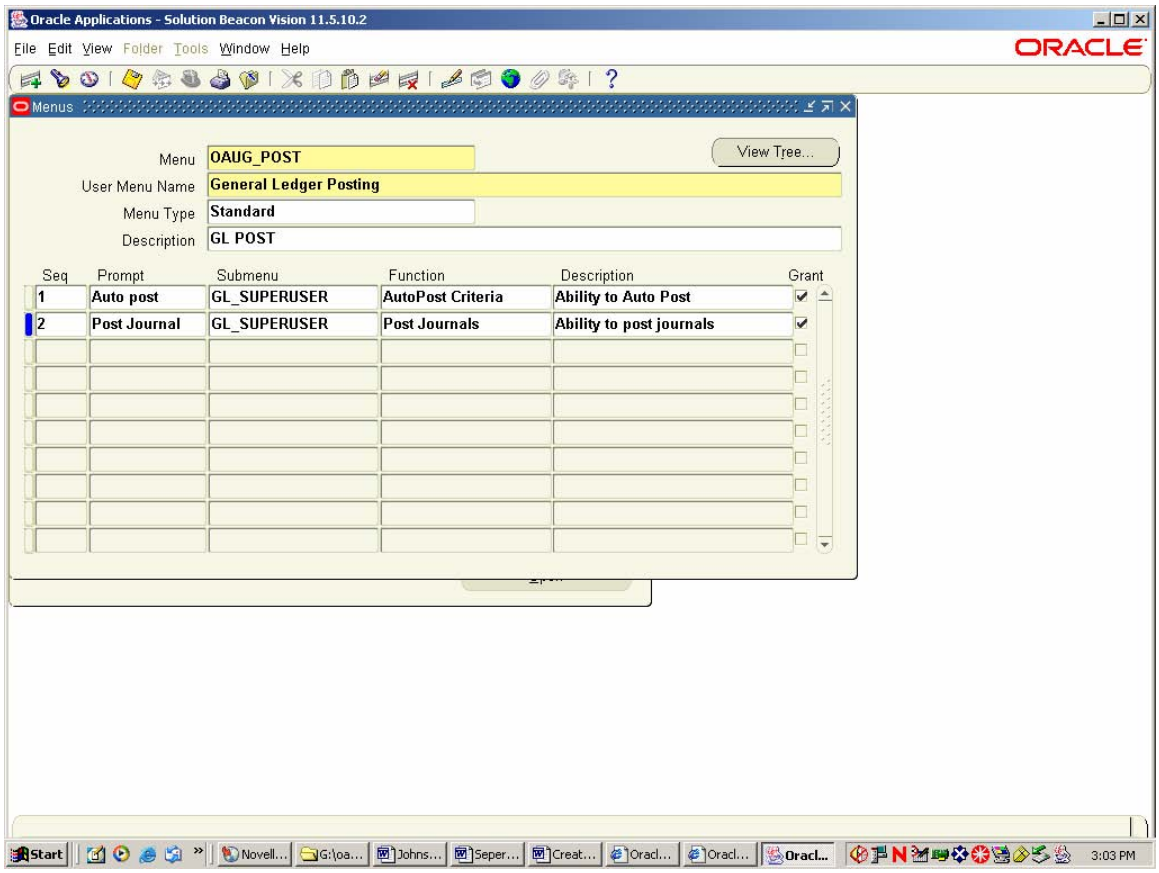
The fields to complete are:

Responsibility = OAUG RESOURCE DIVISION
Application = General Ledger
Responsibility Key = OAUG RESOURCE DIVISION
Description = OAUG RESOURCE DIVISION RESPONSIBILITY
Effective Date = default to start date current date
Data Group
Name = Standard
Application = General Ledger
Menu = GL_SUPERUSER

Select Menu Tab and exclude items you don't want the user to have access too in this case all posting rights.

When I setup the OAUG POST responsibility I basically performed the same steps for OAUG RESOURCE DIVISION with one exception. Instead of excluding Menu items under the Menu tab I created a new Menu. Below is the navigation path to create the new menu:
Navigate ->Application->Menu

COPYRIGHT @ 2008 BY Olga Johnson

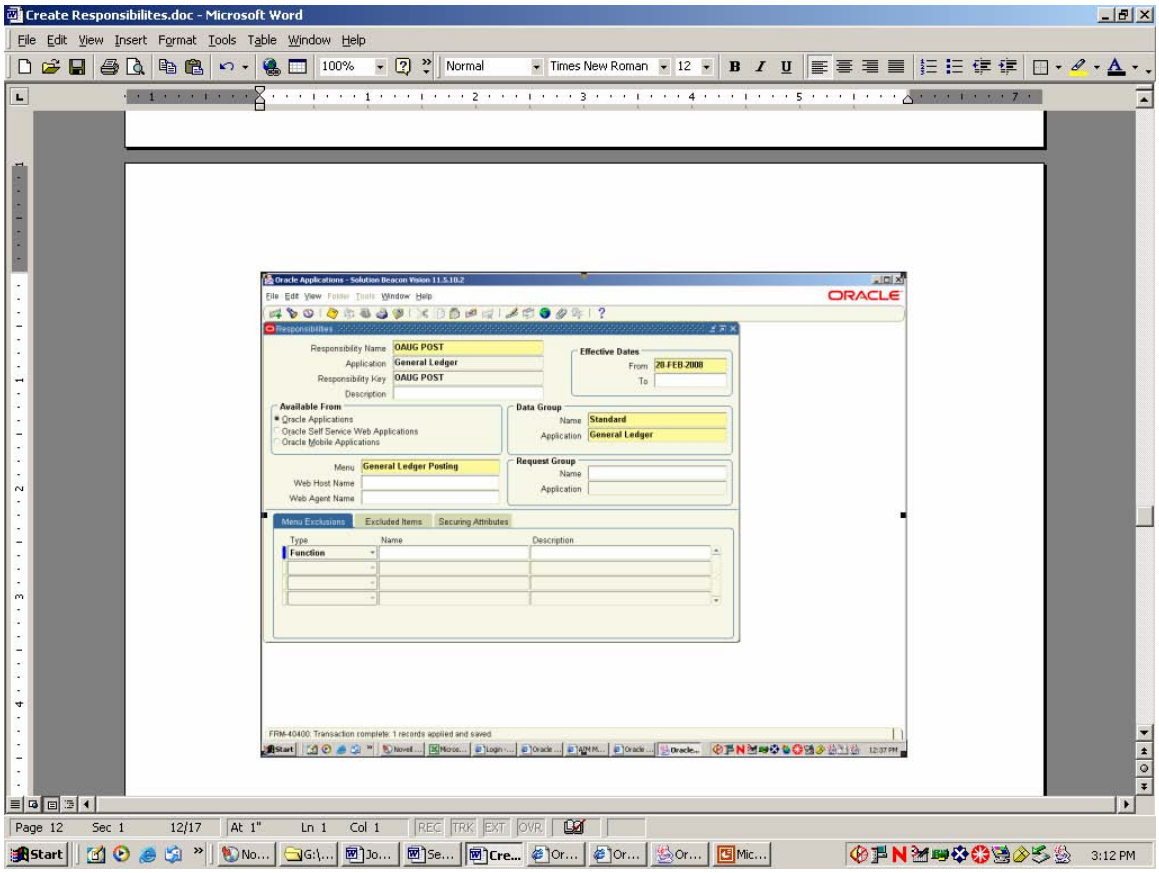


The fields to complete are:

Menu=OAUG POST
User Menu Name = General Ledger Posting
Menu Type= Standard
Description = Optional

Seq 1 Prompt=Autopost Submenu = GL_SUPERUSER Function= AutoPost Criteria
Seq 2 Prompt= Post Journal Submenu = GL_SUPERUSER Function= Post Journal
Description should be filled in.

COPYRIGHT @ 2008 BY Olga Johnson



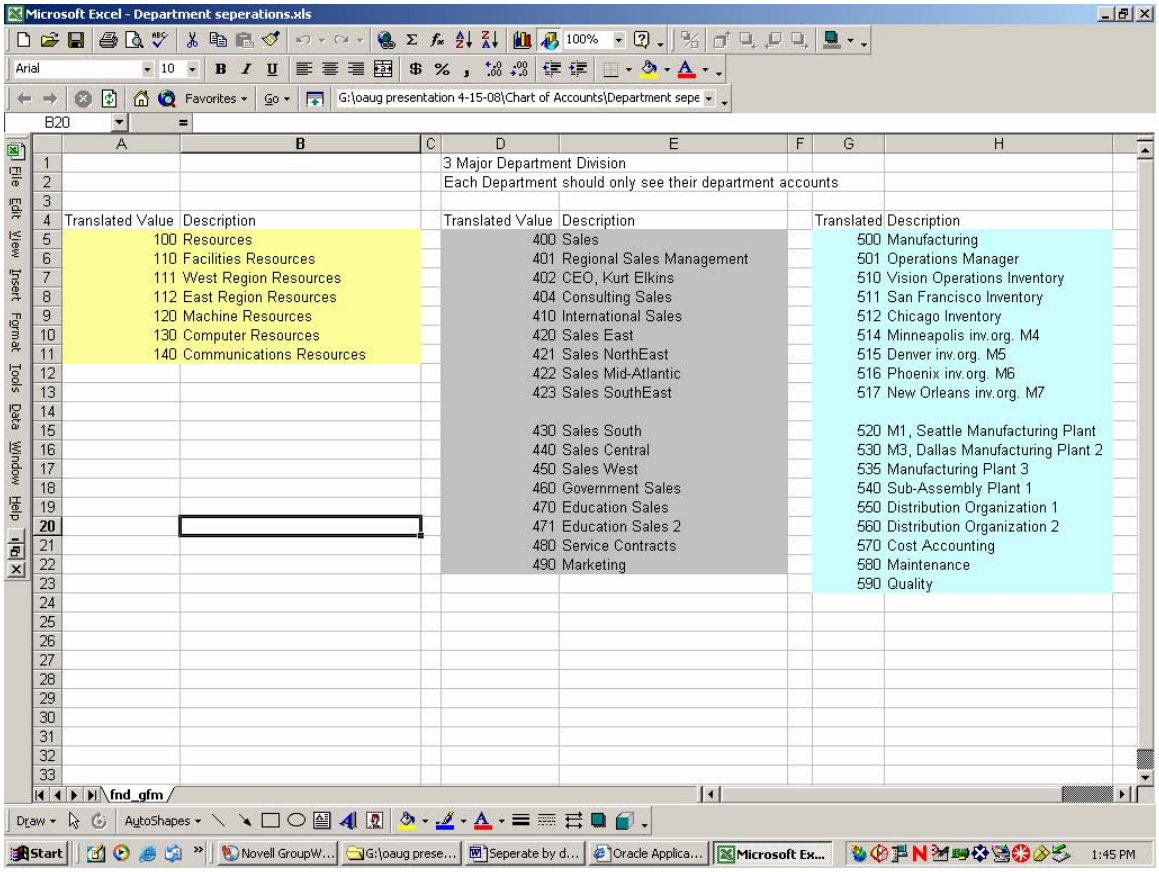
The menu is assigned to the post responsibility in order to allow people with the OAUG Post responsibility to only post journals.

COPYRIGHT @ 2008 BY Olga Johnson

Segment Segregation:

Oracle standard functionality allows the additional security feature of allowing different responsibilities to see only specific segments. To allow for this to be done consistently and easily it would be nice to have numbers in a range represent each for example department.

Below is a chart in solution beacons vision instance:



Microsoft Excel - Department seperations.xls

3 Major Department Division

Each Department should only see their department accounts

Translated Value	Description
100	Resources
110	Facilities Resources
111	West Region Resources
112	East Region Resources
120	Machine Resources
130	Computer Resources
140	Communications Resources

Translated Value	Description
400	Sales
401	Regional Sales Management
402	CEO, Kurt Elkins
404	Consulting Sales
410	International Sales
420	Sales East
421	Sales NorthEast
422	Sales Mid-Atlantic
423	Sales SouthEast
430	Sales South
440	Sales Central
450	Sales West
460	Government Sales
470	Education Sales
471	Education Sales 2
480	Service Contracts
490	Marketing

Translated	Description
500	Manufacturing
501	Operations Manager
510	Vision Operations Inventory
511	San Francisco Inventory
512	Chicago Inventory
514	Minneapolis inv.org. M4
515	Denver inv.org. M5
516	Phoenix inv.org. M6
517	New Orleans inv.org. M7
520	M1, Seattle Manufacturing Plant
530	M3, Dallas Manufacturing Plant 2
535	Manufacturing Plant 3
540	Sub-Assembly Plant 1
550	Distribution Organization 1
560	Distribution Organization 2
570	Cost Accounting
580	Maintenance
590	Quality

In this chart all department segments beginning with '1' represent resources, all department segments beginning with '4' represent sales and all department segments beginning with '5' represent manufacturing. In order to setup the division you would utilize the General Ledger module. The navigation path is:

Navigate ->Setup->Financials->Flex fields->Validation->Security->Define

Step 2: Check Value Set, Name=Department, Click find

Step 3: Add Security Rule Name, Description and message

Step 4: Add Security Rule Elements

a. Include everything in this case 0000 to 9999
b. Exclude low range in this case 0000 to 0099
c. Exclude high range in this case 0200 to 9999

Step 5: Click Assign button

a. Application=General Ledger
b. Responsibility = OAUG Resource Division
c. Name = OAUG Resource

COPYRIGHT @ 2008 BY Olga Johnson

Identity Management:

Oracle Identity Management is a package of products that may have overlapping functions. It allows the management of identities across all enterprise resources on both sides of the firewall. Identity Management is part of Oracle Fusion Middleware products and some of them are:

Identity Federation is a server that allows single sign on capability. You can even have the same sign on across multiple companies. Several tools are provided in Identity Federation such as domain authentication and identification of ID's

Web Access Manager provides tools such as Authentication validating a user's identity in the form of Userid / password to token cards, and bio-metrics.

Web Service Manager provides a method for audit records and data to be place in a commons area for all web service applications. One policy can be applied to multiple web applications also. Four components make up Web Service Manager: 1. Web Service Policy Manager is a graphical tool that allows the creation and versioning of security. 2. Web Services management Gateway acts as a proxy to service clients and routes messages across formats or protocols. 3. Web Services Management Agent is similar to gateway except it is installed into the same process space as the service it is protecting therefore unlike gateway it can encrypt message to the endpoint. 4. Web Service Monitor is a dashboard where statistics such as new policies, service levels and alerts are reported.

Enterprise Single sign-on uses LDAP directory, Active Directory or any SQL database server as its user profile and credential repository. It securely uses a single login credential to most web-based, client-server and legacy applications. Password management can work thru Microsoft windows though secure, flexible, self-service interfaces. It utilizes provisioning and authentication to prove easy use and security.

Identity Manager some of the features of this portion of Identity Manager is it allows the user to manage there own passwords reducing help desk calls for forgotten passwords. Allows the delegation of rule and roles temporarily or permanently.

Access Manager provides centralized authentication, authorization and auditing . Legacy and custom applications can also be authenticated along with Oracle applications using this tool. You can determine hierarchies and flows of authentication. For auditing purposes this provides detail logs of events. Critical contextual events to be reported on can be defined by the user.

Virtual Directory utilizes standards that allow it to speak to other systems easily, works as a firewall, creates virtual views to provide information to other systems without replication, provides a complete view of a person's identity record. Virtual Directory is easy to manage from a desktop-based, graphical user interface client.

Internet Directory supports access control policies, secure authentication mechanism, encrypted attributes, password polices and protects data from privileged users. Database vault is actually a part of Internet Directory.

Audit Vault:

Audit Vault is a single audit data warehouse that is secure, scalable, reliable, and highly available. Audit Vault allows the consolidation of data across enterprises, protects this data through user settings and detect and report on changes to the system.

Database Vault:

Database Vault allows you to set parameters and restrict what different IT professionals can see in your database and still allow IT professionals to perform their work functions. For example, you can limit the time of day a IT worker can make changes, Encrypt data that they have access too and report when they create new users or responsibilities. The database can be partition given various IT professionals access to particular realms.

Oracle Release 12:

A drilldown profile option can apply transaction security in such a way that the sub ledger security can be enforced across the application. Thus drilldown can be restricted to the operating units to which the responsibility has access.

New profile options are in release 12 for journal import:

COPYRIGHT @ 2008 BY Olga Johnson

1. SLA: Disable Journal Import set to No (this is the default and Oracle says to NEVER change the default of this profile option. If an import fails this will call data to be rolled back to the sub ledger therefore you will not have incorrect information on the GL Interface table. Thus all corrections will have to be made in the Sub ledger. Setting this profile option to "Yes" is not supported by Oracle.
2. Also you have additional options for transferring data from payables:
    i. Draft - SLA journals are drafts and can be modified
    ii. Final – SLA journals are Final and cannot be modified
    iii. Final Post – SLA Creates the journal and triggers the General Ledger to post the journal.

Conclusion:

You can increase your compliance now by planning how you want your organization segregated and who you want to see what. You can run reports to provide updates on internal controls readily. Oracle offers products now and continually develop new ones to meet the needs of SOX and other regulations.

COPYRIGHT @ 2008 BY Olga Johnson