R12 Function and Data Security - UMX and Role Based Access Control

Presented By
Susan Behn
VP, Oracle Practice
Agenda

- User Management Layers
- AOL Function and Data Security
  - New Read-only Diagnostic Function Security in 12.1.3
- Role Based Access Control Overview
- Building Blocks for User Management
- Modeling Security Policy Examples
- Delegated Administration
- Provisioning
- Self Service & Approvals
- Proxy Users
- References
User Management Layers

- Core security – levels 1 – 2 is accomplished through AOL or with grants and permissions
- Core security – levels 3 is required for some apps
- Administrative features – levels 4 – 6 are optional

<table>
<thead>
<tr>
<th>Administrative Features</th>
<th>Core Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Self Service &amp; Approvals</td>
</tr>
<tr>
<td>5</td>
<td>Provisioning Services</td>
</tr>
<tr>
<td>4</td>
<td>Delegated Administration</td>
</tr>
<tr>
<td>3</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>2</td>
<td>Data Security</td>
</tr>
<tr>
<td>1</td>
<td>Function Security</td>
</tr>
</tbody>
</table>

6 User access requests with AME Approval Processes
5 Registration processes
4 Administer functions/data for specific groups
3 Grant access to roles that include function/data security
2 What data can a user see
1 What can a user do
AOL Function and Data Security

- Responsibilities are the intersection of the following:
  - Menu (authorizes executable functions)
  - Data Group (authorizes schemas)
  - Request Group (authorizes concurrent programs)
    - Not used by OAF
  - Allows for submenus and functions to be included/excluded

Executable function – Access to User → Define form
Abstract function – Add user or modify user
Read-Only Diagnostics in 12.1.3

- Function security through menus is still a significant piece of the puzzle

**LOOK WHATS NEW!**

- Set profile option “Hide Diagnostics Menu Entry” to “No”
- Assign one or more of the read only subfunctions to the menu where this functionality is needed
- Apps password will not be requested in read-only mode

<table>
<thead>
<tr>
<th>Function Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>FND Diagnostics Menu</td>
<td>Read only for Help → Diagnostics →</td>
</tr>
<tr>
<td>Examine Read Only</td>
<td>Examine</td>
</tr>
<tr>
<td>FND Diagnostics Personalize Read Only</td>
<td>Read only for Help → Diagnostics → Custom Code</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>FND Diagnostics Values Read Only</td>
<td>Read only for Help → Diagnostics → Properties</td>
</tr>
</tbody>
</table>
Read-Only Diagnostics 12.1.3

- Example - Payables, Vision Operations (USA) responsibility linked to menu AP_NAVIGATE_GUI12
- Leave prompt and Submenu null

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Submenu</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FND Diagnostics%Read%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Function Name</th>
<th>Function Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FND Diagnostics Menu Examine Read Only</td>
<td>FND_DIAGNOSTIC...</td>
<td>This permission is used...</td>
</tr>
<tr>
<td>FND Diagnostics Personalize Read Only</td>
<td>FND_DIAGNOSTIC...</td>
<td>This permission is used...</td>
</tr>
<tr>
<td>FND Diagnostics Values Read Only</td>
<td>FND_DIAGNOSTIC...</td>
<td>This permission is used...</td>
</tr>
</tbody>
</table>
Role Based Access Control

- **RBAC** – The RBAC standard supports the mapping of user access control based upon a user’s role in the organization rather than their unique identity
  - **Roles** – a grouping of all the responsibilities, lower level permissions (functions), permission sets, and data security rules that a user requires to perform a specific task
  - **Role Categories** – Organize roles into groups
Examples of Roles

- **Employee**
  - Create Employee role with access to HR self service and iExpenses

- **AP Clerk**
  - Grant Employee role
  - Grant AP Clerk role with access to AP clerk functions

- **Sales Rep**
  - Grant Employee role
  - Grant Sales role with access to sales functions

- **AP Supervisor**
  - Grant Employee Role
  - Grant AP Clerk Role
  - Grant AP Manage role with access to AP Manger functions
Components by Responsibility

- System Administrator Responsibility
  - Manage responsibilities and related objects

- User Management – Layers 3 and up

- Functional Administrator Responsibility
  - Function Security Layer

- Functional Developer Responsibility
  - Data Security Layer
User Management Building Blocks

- **Objects**
  - Define data to be secured – a table or view
  - Stored in FND_OBJECTS, FND_OBJECTS_TL

- **Object Instance Sets**
  - The “WHERE” clause for an object
  - Stored in FND_OBJECT_INSTANCE_SETS, FND_OBJECT_INSTANCE_SETS_TL

- **Managed in Functional Developer Responsibility**
User Management Building Blocks

- Permissions – 2 types – function and data
  - Function Security Permissions – control access to abstract functions
    - Examples
      - Executable function is access to User Management → Roles & Role Inheritance Form
      - Abstract functions defined as role permissions
        - Create Role – Assign Role
        - Manage Role – Revoke Role
  - Data Security Permissions – control access to objects
    - Data limited by where clause
    - Stored in FND_FORM_FUNCTIONS, FND_FORM_FUNCTIONS_TL
User Management Building Blocks

- Permission Sets
  - Grouping of permissions
    - Example: All User Administration Privileges
  - A permission set can contain other sets
  - Stored in FND_MENUS, FND_MENUS_TL, FND_MENU_ENTRIES, FND_MENU_ENTRIES_TL
User Management Building Blocks

- **Grants**
  - Provide permissions for actions on a specified object
    - Attach function permissions and data permissions (data security polices) to grantee

- **Grantee**
  - Who gets the grant
    - A role or group
    - A specific user
    - All Users

- **Data Security Policy**
  - Grant that includes both an object and permission set

- **Stored in FND_GRANTS**
STACKING UP THE BUILDING BLOCKS
Modeling Security Policies

1. Step 1 – Assign access to user management to appropriate users
2. Step 2 – Identify or create permissions that group functions (function security)
3. Step 3 – Identify product seeded objects / object instance sets (data security)
4. Step 4 – Identify seeded grants / create grants
5. Step 5 – Create roles / Identify seeded roles
GRANT ACCESS TO USER MANAGEMENT TO APPROPRIATE USER(S)
Managing Users – Step 1

- By default, only Sysadmin has access to User Management
- Assign a user management role to the appropriate user

![User Management Interface]

- Search for user
- Click pencil to edit
Managing Users – Step 1

- Click the “Assign Roles” button to add a role

Click assign roles and then click the apply button
Managing Users – Step 1

- Search for the “Security Administrator” Role, check the box and click select
  - Customer Administrator – manage users with party type = customer
  - Partner Administrator – manage users with party type = partner

Other seeded security roles include Customer Administrator and Partner Administrator
Managing Users – Step 1

- Enter a justification and click “Apply”

User Management responsibility is inherited by assigning this role.
Managing Users – Step 1

- System Administrator → User → Define
- User Management is shown as an indirect responsibility
STEP 2
IDENTIFY SEEEDED PERMISSIONS
CREATE PERMISSIONS
 Permissions

- To demonstrate function security, Approvals Management will be used as the example.
- A user will be given access to perform all functions in approvals management.
- To gain familiarity with permissions available:
  - Go to Functional Administrator → Permissions to search for seeded permissions.
There are 16 permissions available for AME.
Click the update button to examine the “AME Action Create” Permission.
Permissions

- This permission belongs to one permission set with the same name as the permission.
Examine the permission set by selecting the permission set in the permission set tab and clicking the update button.
Permission Set

- Notice the AME Action Create includes more than one permission
  - Grants are to permission sets – not to permissions
    - Become familiar with the security hierarchy
    - Working with seeded permission, permission sets and other seeded user management components are a good way to learn user management concepts

<table>
<thead>
<tr>
<th>Focus Name</th>
<th>Permission Set</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AME Action Create</td>
<td>AME_ACT_CREATE_PERM_SET</td>
<td>AME_REG_ACTION_CREATE</td>
<td>AME Action Create</td>
</tr>
<tr>
<td>AME Regular Action Create</td>
<td>AME_REG_ACTION_CREATE</td>
<td>AME_REG_ACTION_CREATE</td>
<td>AME Regular Action Create</td>
</tr>
<tr>
<td>AME Action Create</td>
<td>AME_ACT_CREATE_PERMISSION</td>
<td>AME_ACT_CREATE_PERMISSION</td>
<td>AME Action Create</td>
</tr>
</tbody>
</table>
In our example, we want the user to have access to ALL functions the transaction type “AP Invoice Approval”

The permission set for all AME functions is “AME All Permission Sets”

- Note that this permission set includes other permission sets

<table>
<thead>
<tr>
<th>Focus Name</th>
<th>Permission Set</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AME All Permission Sets</td>
<td>AME_ALL_PERM_SETS</td>
<td></td>
<td>AME All Permission Sets</td>
</tr>
<tr>
<td>AME Attribute Modifier</td>
<td>AME_ATR_MODIFY_PERM_SET</td>
<td></td>
<td>AME Attribute Modifier</td>
</tr>
<tr>
<td>AME Condition Modifier</td>
<td>AME_CON_MODIFY_PERM_SET</td>
<td></td>
<td>AME Condition Modifier</td>
</tr>
<tr>
<td>AME Action Type Modifier</td>
<td>AME_ATY_MODIFY_PERM_SET</td>
<td></td>
<td>AME Action Type Modifier</td>
</tr>
<tr>
<td>AME Action Modifier</td>
<td>AME_ACT_MODIFY_PERM_SET</td>
<td></td>
<td>AME Action Modifier</td>
</tr>
<tr>
<td>AME Action Type Config Modifier</td>
<td>AME_ATY_CONFIG_MODIFY_PERM_SET</td>
<td></td>
<td>AME Action Type Config Modifier</td>
</tr>
<tr>
<td>AME Approver Group Modifier</td>
<td>AME_APPG_MODIFY_PERM_SET</td>
<td></td>
<td>AME Approver Group Modifier</td>
</tr>
<tr>
<td>AME Rule Modifier</td>
<td>AME_RULE_MODIFY_PERM_SET</td>
<td></td>
<td>AME Rule Modifier</td>
</tr>
<tr>
<td>AME Test Modifier</td>
<td>AME_TEST_MODIFY_PERM_SET</td>
<td></td>
<td>AME Test Modifier</td>
</tr>
<tr>
<td>AME Admin Modifier</td>
<td>AME_ADNUMODIFY_PERM_SET</td>
<td></td>
<td>AME Admin Modifier</td>
</tr>
<tr>
<td>AME Business Dashboard Viewer</td>
<td>AME_BUS_DASHBOARD_PERM_SET</td>
<td></td>
<td>AME Business Dashboard Viewer</td>
</tr>
<tr>
<td>AME Setup Report Viewer</td>
<td>AME_SETUP_REPORT_PERM_SET</td>
<td></td>
<td>AME Setup Report Viewer</td>
</tr>
<tr>
<td>AME Exceptions Log Viewer</td>
<td>AME_EXCEPTIONS_LOG_PERM_SET</td>
<td></td>
<td>AME Exceptions Log Viewer</td>
</tr>
<tr>
<td>AME Config Variable Viewer</td>
<td>AME_CFV_TT_SPECIFIC_PERM_SET</td>
<td></td>
<td>AME Config Variable Viewer</td>
</tr>
<tr>
<td>AME Config Default Modifier</td>
<td>AME_CFV_DEFAULT_PERM_SET</td>
<td></td>
<td>AME Config Default Modifier</td>
</tr>
<tr>
<td>AME Calling Applications</td>
<td>AME_TRANS_TYPE_DATA_PERM_SET</td>
<td></td>
<td>AME Calling Applications</td>
</tr>
</tbody>
</table>
STEP 3
SEED OBJECTS
Seeded Objects

- To demonstrate data security, Approvals Management will be used again as the example.
- A user will be given access to manage the approval process for the payables invoice approval.
- Go to Functional Developer → Objects to search for available seeded objects.
- If an object is not available, you can create objects.
Seeded Objects

Tip: Query by responsibility to get familiar with what is seeded

Click update to view details but avoid changing seeded objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Code</th>
<th>Application Name</th>
<th>Database Object</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>AME Transaction Types</td>
<td>AME_TRANSACTION_TYPES</td>
<td>Human Resources</td>
<td>AME_CALLING_APPS</td>
<td>01-Aug-2005</td>
</tr>
<tr>
<td>HR_ALL_ORGANIZATION联合国</td>
<td>HR_ALL_ORGANIZATION_UNITS</td>
<td>Human Resources</td>
<td>HR_ALL_ORGANIZATION_UNITS</td>
<td>19-Jan-2006</td>
</tr>
<tr>
<td>Persons Legislation</td>
<td>HR_PERSON_LEGISLATION</td>
<td>Human Resources</td>
<td>HR_PERSON_LEGISLATION_V</td>
<td>26-Mar-2002</td>
</tr>
</tbody>
</table>
Seeded Objects

- Two columns are included which can be used to limit access

Note the Object Instance Sets Tab and Grants Tab
Seeded Objects

- Click on the Object Instance Set tab for this object to view the where clause

- The predicate allows the user to enter the parameters to select the application and transaction type in the grant
STEP 4
IDENTIFY SEEDED GRANTS
CREATE GRANTS
Grants

- Create the grant to allow sbehn to perform all AME function for the payables invoice approval transaction type
- Click on grant tab

Notice this takes you to the same form as you see in the Functional Administrator responsibility
- We are going to enter an object to establish a Data Security Policy
Grants

- Enter name, description, grantee type, grantee
- Enter the object name
- Click Next
Grants

- Choose the context to limit rows
  - For this example, choose instance set
Grants

- We already determined there was an “AME Transaction Type” Instance Set
- Chose this value and Click Next
Grants

- Now enter the values for the parameters we saw earlier in the object instance set
- The predicate is displayed for reference
  - Parameter 1 is the application
  - Parameter 2 is the AME transaction type
Grants

- Scroll down and choose the functions the grantee will be allowed to execute for this group of data by selecting the permission set “AME All Permission Sets”
Grants

- The final page is a review page
- Click finish and the confirmation page will appear
- Now you have access to data and functions you can perform on that data
- Click OK
Role Based Access Control

- In step 1, we gave someone access to user management.
- In step 2, we identified the “AME All Permission Sets” to provide function security.
- In step 3, we identified the “AME Transaction Types” object to provide data security.
- In step 4, we joined the function and data security together in a grant to allow SBEHN to perform all functions for AME for Payables Invoice Approvals.
- But...the user still doesn’t have access yet to the responsibility used to manage AME.
STEP 5
CREATE ROLE CATEGORIES
CREATE ROLES
ASSIGN RESPONSIBILITIES TO ROLES
Assign Roles

- Assign AME roles to SBEHN the same way we assigned the “Security Administrator” role
- Query the user and click the pencil
Click the “Assign Roles” button
Seeded Roles

- Choose the “Approvals Management Administrator” role and provide justification
- Grants multiple roles and 2 responsibilities
FULL UTILIZATION OF RBAC
ROLE CATEGORIES
CREATING ROLES FOR RESPONSIBILITIES
### Role Categories

- **User Management ➔ Role Categories**

---

#### User Management

<table>
<thead>
<tr>
<th>Users</th>
<th>Roles &amp; Role Inheritance</th>
<th>Role Categories</th>
<th>Registration Processes</th>
<th>Security Report</th>
</tr>
</thead>
</table>

#### View Lookup Type: Role Categories

- **Name**: User Management : Role Categories
- **Code**: UMX_CATEGORY_LOOKUP
- **Description**: User Management : Role Categories. TAG *must* be defined as "ACCESS_ROLES"
- **Application Name**: Application Object Library
- **Access**: Extensible

#### Lookup Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
<th>Description</th>
<th>Tag</th>
<th>Effective From</th>
<th>Effective To</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAGNOSTICS.Roles</td>
<td>Diagnostics Roles</td>
<td>List of seeded Diagnostics Roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFORMATION.Technology</td>
<td>Information Technology</td>
<td>Information Technology related roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MISC</td>
<td>Miscellaneous</td>
<td>Miscellaneous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTA.Training</td>
<td>Training</td>
<td>Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECURITY.Admin</td>
<td>Security Administration</td>
<td>Roles which provide access to features related to Security Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TERR.MGMT.Job.Roles</td>
<td>Territory Management Job Roles</td>
<td>Territory Management Job Roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TERR.MGMT.Task.Roles</td>
<td>Territory Management Task Roles</td>
<td>Territory Management Task Roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Click Update Button**
## Role Categories

### User Management

<table>
<thead>
<tr>
<th>User Management: Role Categories</th>
<th>Role Categories</th>
<th>Registration Processes</th>
<th>Security Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Lookup Type:</strong> Role Categories</td>
<td><strong>Indicates required field</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Name</td>
<td>User Management : Role Categories</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Code</strong></td>
<td><strong>UMX Categoria LOOKUP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>User Management : Role Categories. TAG <em>must</em> be defined as &quot;ACCESS_ROLES&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application Name</strong></td>
<td>Application Object Library</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>Extensible</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Lookup Codes

<table>
<thead>
<tr>
<th>Select Code</th>
<th>Meaning</th>
<th>Description</th>
<th>Tag</th>
<th>Effective from</th>
<th>Effective to</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAGNOSTICS_ROLES</td>
<td>Diagnostics Roles</td>
<td>List of seeded Diagnoses</td>
<td></td>
<td>12-Mar-2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFORMATION_TECHNOLOGY</td>
<td>Information Technology</td>
<td>Information Technology</td>
<td></td>
<td>01-Jan-2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MISC</td>
<td>Miscellaneous</td>
<td>Miscellaneous</td>
<td></td>
<td>31-Dec-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTA TRAINING</td>
<td>Training</td>
<td>Training</td>
<td></td>
<td>05-Jul-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECURITY_ADMIN</td>
<td>Security Administration</td>
<td>Roles which</td>
<td></td>
<td>31-Dec-2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TERR_MGMT_JOB_ROLES</td>
<td>Territory Management</td>
<td>Territory Management</td>
<td></td>
<td>19-Oct-2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TERR_MGMT_TASK_ROLES</td>
<td>Territory Management</td>
<td>Territory Management</td>
<td></td>
<td>19-Oct-2005</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Click Add Another Row

---

![Infosemantics, Inc.](image)
Add a category to help organize your roles

Click Apply
Create Role

- User Management ➔ Role & Role Categories

Click Create Role
Create Role

- Select category, provide role code, display name, description and application and click apply.
Create Role

- To add responsibility - re-query role, view in hierarchy, then add node

**Steps:**

1. Click View in Hierarchy
2. Click Add Node
Create Role

- Query the responsibility required, then click the Quick Select icon
Create Role

- Payables Manager role now includes Payables Manager responsibility
- Add other responsibilities as needed

```
<table>
<thead>
<tr>
<th>Focus Name</th>
<th>Code</th>
<th>Application</th>
<th>Active</th>
<th>Update</th>
<th>Add Node</th>
<th>Remove Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Roles, Responsibilities, and Groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payables Manager</td>
<td>UMX</td>
<td>UMX_PAYABLES_MGR</td>
<td>Payables</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payables Manager</td>
<td>FND_RESP</td>
<td>SQLAP</td>
<td>PAYABLES_MANAGER</td>
<td>STANDARD</td>
<td>Payables</td>
<td>✓</td>
</tr>
</tbody>
</table>
Seeded Roles

- Oracle has provided seeded roles for
  - Approvals Management
  - Diagnostics
  - Learning Management
  - Territory Management
  - User Management
  - Integration Repository
  - iReceivables
  - iSetup
  - Integrated SOA Gateway (New)

- To see what’s new after patches, look for roles in User Management responsibility or query WF_ALL.Roles.VL
New Surprises: Access to Integration Repository

- Release 11i
  - Go to My Oracle Support
- Early R12
  - Assign Responsibility – Integrated SOA Gateway
- Release 12.1+
  - Assign one of following roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Code</th>
<th>Application</th>
<th>Status</th>
<th>View In Hierarchy</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Integration Developer</td>
<td>UMX</td>
<td>FND_SYSTEM_INTEGRATION_DEVELOPER</td>
<td>Application Object Library</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>System Integration Analyst</td>
<td>UMX</td>
<td>FND_SYSTEM_INTEGRATION_ANALYST</td>
<td>Application Object Library</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Irep Administrator</td>
<td>UMX</td>
<td>FND_IREP_ADMIN</td>
<td>Application Object Library</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
New Surprises: Access to Concurrent Requests

- Profile Option “Concurrent Report Access Level” is obsolete in 12.1
  - Allowed users to see all concurrent requests in a responsibility
- Replaced by RBAC permissions
  - See My Oracle Support ID 737547.1
DELEGATED ADMINISTRATION
Delegated Administration

- Create local administrators to manage a subset of users and/or roles

- What is required?
  - A role that grants User Management → Users to user who will be delegated administrator
  - Grant of subset of UMX_PERSON_OBJECT defining which users can be administered
  - Grant of permission set with appropriate privileges
    - Query Person Details
    - Edit Person Details
    - Manage User Accounts
    - Reset Passwords
Delegated Administration

- Presentations with good examples
  - Create a role to administer a specific organization
    - Collaborate 2009: *From Responsibilities to Roles: Moving Toward the Role Based Access Control (RBAC) Model*
      - Marquette University
  - Create a junior workflow administrator
    - Collaborate 2009: *What's New in Workflow: 11i RUP5, RUP6 and R12*
      - Karen Brownfield and Susan Behn
PROVISIONING

- Delegated Administration
- Role Based Access Control
- Data Security
- Function Security
Provisioning (Registration)

- Three types supported
  - Self-service account requests – typically invoked from a web page
    - Collections Self Registration
    - iReceivables Self Registration
  - Requests for additional access
    - Employee Registration
  - Account Creation by Administrators
    - Account Creation for Existing Person
      - Automate on-boarding for new employees
Provisioning (Registration)

- Other products also utilize the user management registration engine for registration process, but they access the registration process through their own UI
  - iSupplier
- Consult the implementation guide for those products to utilize those registration processes
- iSupplier users are not created in user management
Provisioning (Registration)

- Update an existing process or duplicate to create new processes
Provisioning (Registration)

- See *Oracle User Management Developer Guide*
- Example – Self Service Account Creation
Provisioning (Registration)

Example – Self Service Account Creation

Create pages to ask all the required questions

Business event which raises a workflow for approval and identify verification notification

Event to invoke custom business logic

AME transaction type to manage approvals
Registration Process Flow
SELF SERVICE AND APPROVALS
Once registration processes are configured, users perform self-service tasks to request access.

Login and click the preferences button in the top right corner.

Click the Access Requests button on the left side of the screen.

- Current roles will be displayed.

Click the Request Access button.
Self Service and Approvals

- Select the role to add and click next

Enter a justification and click next
Self Service and Approvals

- Review and click submit

Note the Warning
- For iReceivables, additional information is required
  - Click on the link to enter the addition information
Self Service and Approvals

- Once all the requested information is entered, the business event will raise the workflow to complete the registration process
MANAGE PROXIES
Proxies

- Proxy authority can be granted to another user for a specific time period
  - Cover vacation/leave of absence
- Delegator grants/revokes proxy privilege to user
- User utilizes “proxy switcher feature” to change roles
- All forms will show proxy mode status
- Audit control - Actions are tracked to show delegate is acting on behalf of delegator
In order to delegate or receive authority, users must have the “Manage Proxies” role

- Query the users, click the pencil to update, click the “Assign Roles” button and add the Manage Proxies role
- Enter a justification and save
Proxies

- Click the preference button
- There is now a new Manage Proxies function

The Add People Button will allow the user to designate a proxy user
Proxies

- Add a user and apply
  - Now the operations user can act on my behalf
  - Set an End Date at this time if this is to cover a fixed vacation period or other leave of absence
- When the operations user is logged in a “Switch User” option will be available
- Notice that the user is currently logged in as OPERATIONS
- Click the Switch icon to switch users
Proxies

- Now there is a “Return to Self” button
- The user is logged in as Operations operating as Proxy for SBEHN
Proxies

- Run the Page Access Tracking Data Migration concurrent program to populate the Proxy Report
  - There are no parameters
- Then go back to Manage Proxies and click the Run Proxy Report Button
Proxies

- The report shows all navigation completed by the proxy user

<table>
<thead>
<tr>
<th>User Name</th>
<th>Responsibility</th>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>LOGIN</td>
<td>24-Jun-2011 18:09:45</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>LOGOUT</td>
<td>24-Jun-2011 18:17:44</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>System Administrator, Vision Insurance (USA)</td>
<td>RESP_CHANGE</td>
<td>24-Jun-2011 18:15:11</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>RESP_CHANGE</td>
<td>24-Jun-2011 18:12:48</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>Invoice Workbench</td>
<td>24-Jun-2011 18:12:49</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>General Preferences</td>
<td>24-Jun-2011 18:16:18</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>Manage Proxies</td>
<td>24-Jun-2011 18:16:21</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>Manage Proxies</td>
<td>24-Jun-2011 18:16:33</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>Proxy Report</td>
<td>24-Jun-2011 18:16:33</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>Payables Manager</td>
<td>Proxy Report</td>
<td>24-Jun-2011 18:16:50</td>
</tr>
</tbody>
</table>
Security Reports

- Reports are available for lists of users, roles/responsibilities, functions and data security objects.
- Reports can be generated in html, excel or pdf.

[Image of a search report interface with options for report type, view as, and security reports-related information.]

[Logos for Infosemantics, Inc. and Oracle Gold Partner are present at the bottom.]
Summary

- RBAC allows organizations to create roles based on job functions
  - Less maintenance after initial setup
  - Better security
- Delegated administration allows organizations to decentralize the management of users
  - Will this help your organization distribute the load of user access assignments more efficiently or provide better security across global organizations?
- Registration processes enable organizations to automate the process to provide user access
  - Think about how much time system administrators or DBAs would save over a period of one year by automating this process
- Self Service requests and approvals allow users to request access
  - Less paper
  - More efficiency
References

- *Oracle Applications System Administrator's Guide - Security*
- See *Oracle User Management Developer Guide*
- My Oracle Support ID: 553547.1 – Data Security Terminology
- My Oracle Support ID: 553290.1 – Introduction to the Grants Security System and Data Security
- E-Business Suite User Management SIG
  - [http://ebsumx.oaug.org/](http://ebsumx.oaug.org/)
About Infosemantics

- Established in 2001
- Commercial, Higher Education, and Federal Government client base
- Senior resources averaging 15 years of experience
Thank You!

Susan Behn
susan.behn@infosemantics.com

www.infosemantics.com
People First. Driving Solutions Together®