



Administration of Users, Roles and Responsibilities in Release 12 – When Technologies Collide

Chuck Kennedy

Susan Behn

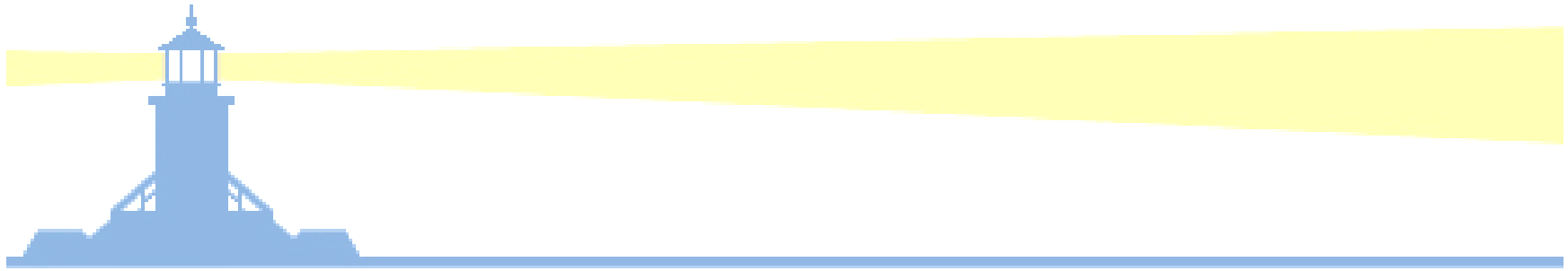
Brian Bent

April 15, 2008


ORACLE CERTIFIED ADVANTAGE
PARTNER



SOLUTION BEACON, LLC
Real Solutions for the Real World®



Role Based Access Control (RBAC)



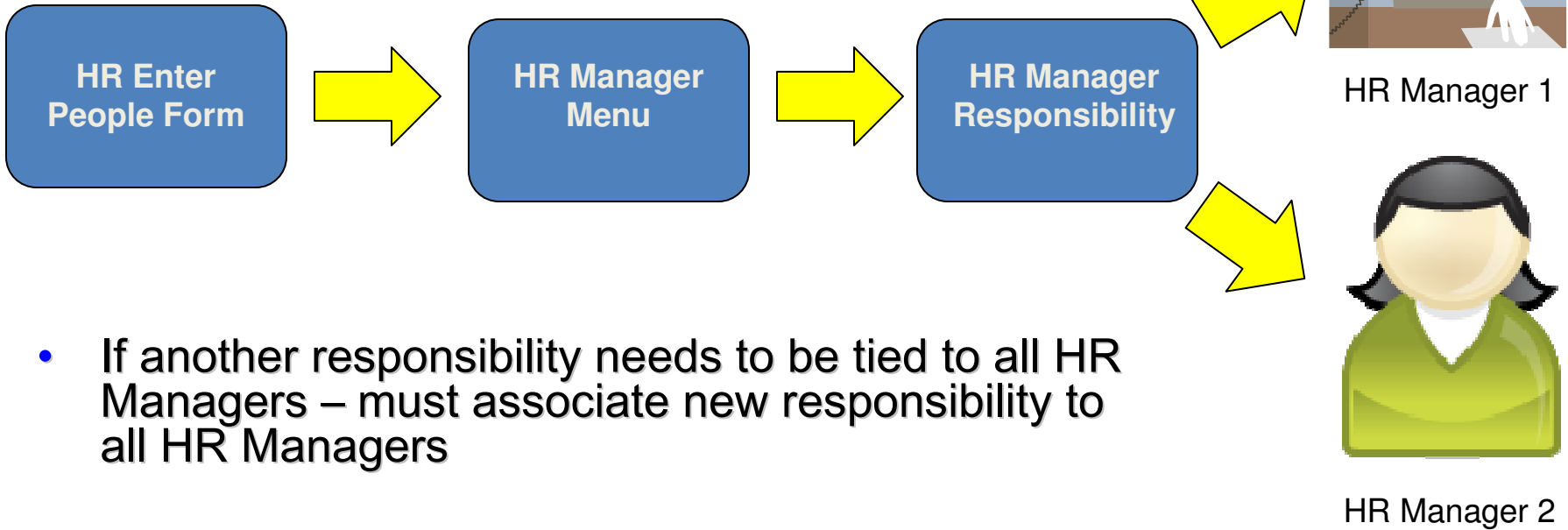
Role Based Access Control (RBAC)

- What is RBAC?
 - MetaLink Doc. ID: 290525.1 “Role Based Access Control (RBAC) is an ANSI standard (ANSI INCITS 359-2004) supported by the National Institute of Standards & Technology (NIST).
 - The RBAC standard supports the mapping of user access control based upon a user’s role in the organization rather than their unique identity
 - Responsibilities aggregate menus/functions for navigation
 - Roles correlate functions to specific data access
 - Role inheritance reduces user administration



Oracle Forms User Provisioning

- Responsibilities are associated with individual users

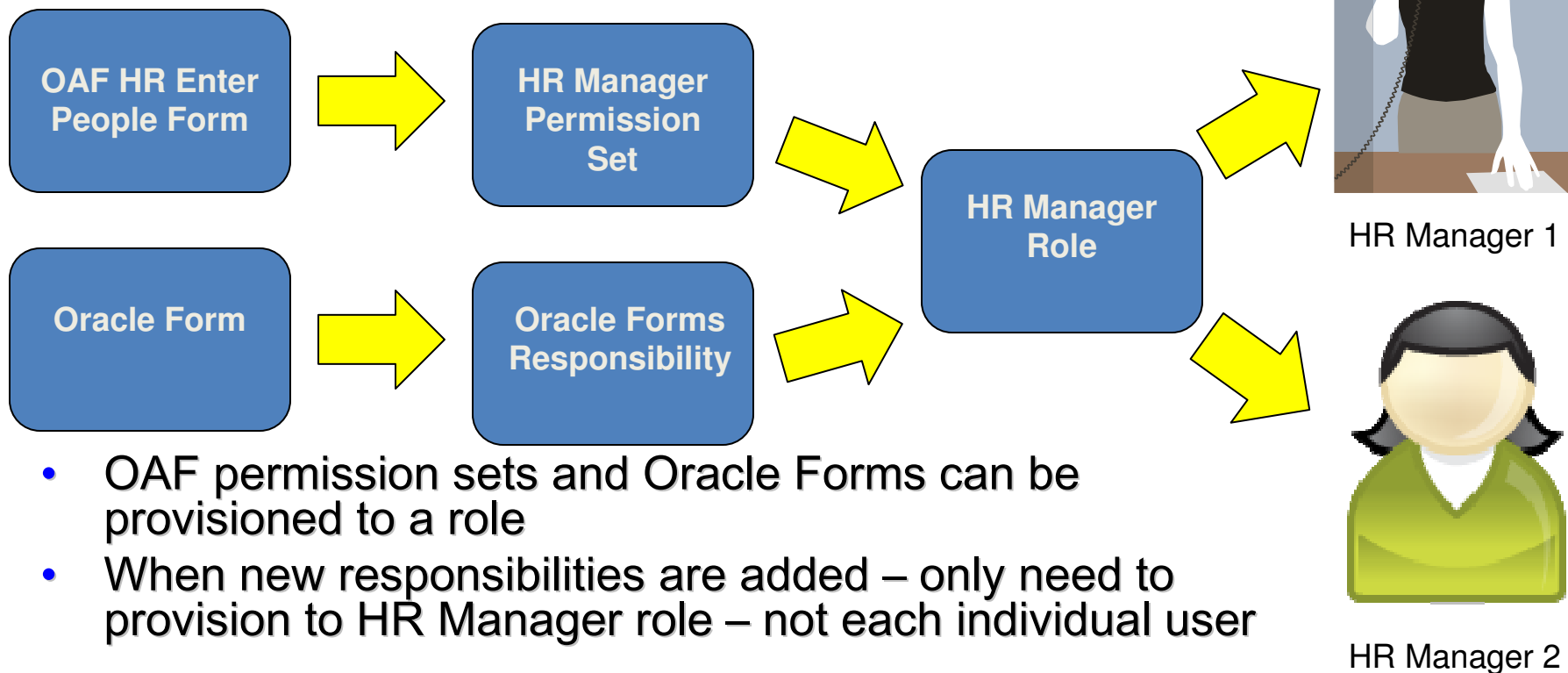


- If another responsibility needs to be tied to all HR Managers – must associate new responsibility to all HR Managers



Oracle Application Framework User Provisioning

- Roles are associated with individual users
- Supports RBAC standard of role based provisioning

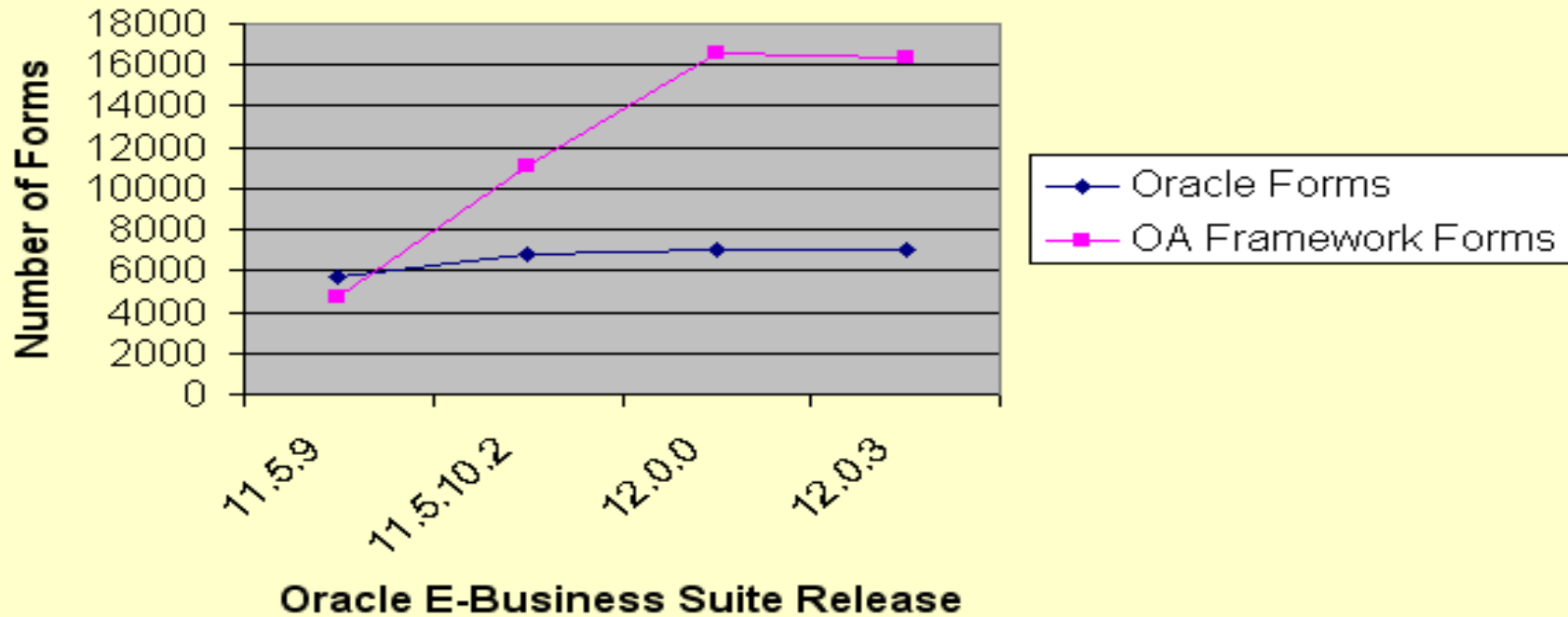


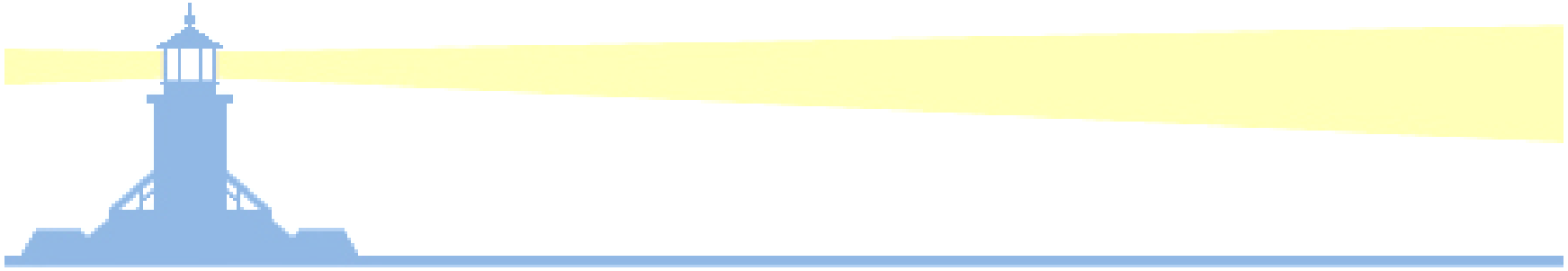
- OAF permission sets and Oracle Forms can be provisioned to a role
- When new responsibilities are added – only need to provision to HR Manager role – not each individual user



Pervasiveness of OA Framework

E-Business Suite Registered Forms





Oracle User Management





Oracle User Management

- Role Design, Creation and Assignment
- Registration Processes
- Manage Proxies
- Product Family Functionality



Oracle User Management

- Grants
 - Grant specific users to roles and/or responsibilities
 - Grant specific users to Data Security Policies
- Data Security Policies
 - Regulates specific data accesses – can be for specific columns (data instance) or a group of rows (instance set)
- Registration Processes
 - New user registration integrates with AME for approvals
 - Default registration policy is “email”
 - That’s why Self-Service userids are usually email addresses

Initial Grant

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'Object Details' page for 'UMX - System Administrator - All Roles Grant'. The browser's address bar shows the URL: http://vis1200int1.solutionbeacon.net/OA_HTML/OA.jsp?page=/oracle/apps/fnd/security/objects. The page content includes a table with the following data:

Name	Grantee	Valid from	Valid to	Set	Data Context Type	Instance Set
Role Administration privileges.	Group Of Users	10-Aug-2004		Assign / Revoke Role	All Rows	
UMX - System Administrator - All Roles Grant	Specific User	28-Jun-2004		Assign / Revoke Role	All Rows	
Role Administration privileges.	Group Of Users	05-Jul-2005		Assign / Revoke Role	Instance	
Role Administration privileges.	Group Of Users	04-Aug-2004		Assign / Revoke Role	Instance	
Role Administration privileges.	Group Of Users	04-Aug-2004		Assign / Revoke Role	Instance	
Role Administration privileges.	Group Of Users	31-Oct-2005		Assign / Revoke Role	Instance	

Below the table, there are buttons for 'Update' and 'Delete', and a 'Return to Object Search' link. The footer of the page includes 'About this Page', 'Privacy Statement', 'Security', 'Core Services', 'Home', 'Logout', 'Preferences', 'Diagnostics', and 'Copyright (c) 2006, Oracle. All rights reserved.'

- Default User Management provisioning is granted to SYSADMIN userid
- Must login as SYSADMIN and grant User Management role to group of users or specific user





Initial Grant

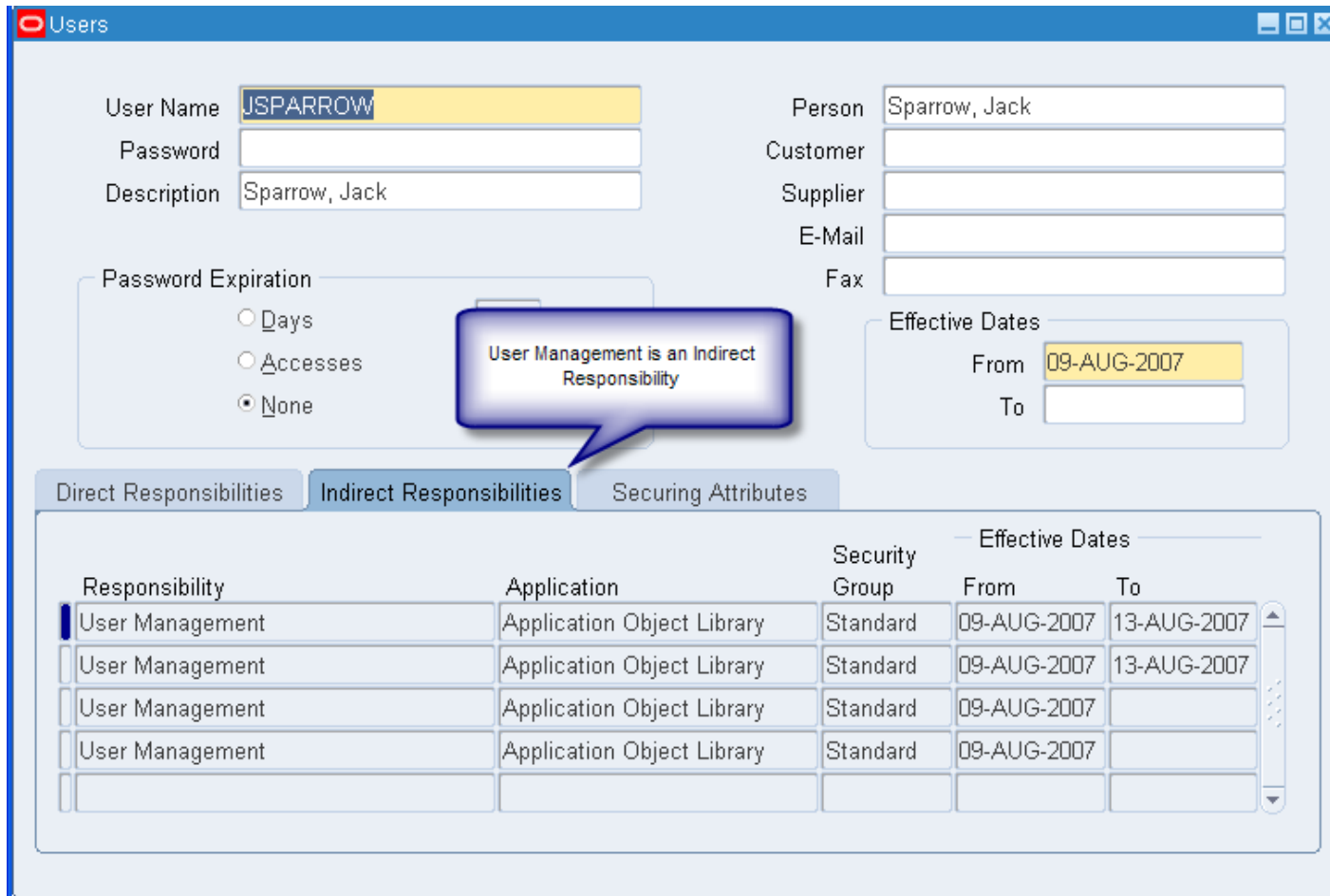
Details	Role	Description	Status
+ Show	SB_CK_SPECIFIC_LE_VISION_JAPAN	SB_CK_SPECIFIC_LE_VISION_JAPAN	Assigned
- Hide	- Hide Security Administrator	Security Administrators manage all user accounts in the system, and can assign / revoke all roles. Security Administrators also manage system accounts (such as GUEST), that are not tied to a person.	
	* Active From <input type="text" value="30-Apr-2007"/> Active To <input type="text"/>		
	Role Inheritance User Management, Manage Proxies		
+ Show		without sharing your password.	
+ Show	Territory Reports View Operation	Territory Reports View Operation	Assigned
+ Show	Matching Attributes Enabling	Matching Attributes Enabling	Assigned
+ Show	Named Account Management (Admin)	Named Account Management (Admin)	Assigned
+ Show	Sales Team Search	Sales Team Search	Assigned
- Hide	- Hide User Management	User Management	
Inherited	Inherited roles can only be revoked through the originating roles below.		
Inherited	Inherited From Security Administrator		
+ Show	Territory Maintenance	Territory Maintenance for all Usages	Assigned

Must grant the seeded Security Administrator role

Role inheritance provides the User Management role



Indirect Responsibility



























The screenshot shows the Oracle Users form for user JSPARROW. The form includes fields for User Name, Password, Description, Person, Customer, Supplier, E-Mail, and Fax. A callout box points to the Indirect Responsibilities tab, stating "User Management is an Indirect Responsibility". The Indirect Responsibilities tab is active, showing a table of responsibilities.

Responsibility	Application	Security Group	Effective Dates From	Effective Dates To
User Management	Application Object Library	Standard	09-AUG-2007	13-AUG-2007
User Management	Application Object Library	Standard	09-AUG-2007	13-AUG-2007
User Management	Application Object Library	Standard	09-AUG-2007	
User Management	Application Object Library	Standard	09-AUG-2007	

- Shows as indirect responsibility on System Administrator user form
- Held in WF_ROLES and WF_USER_ROLE_ASSIGNMENTS

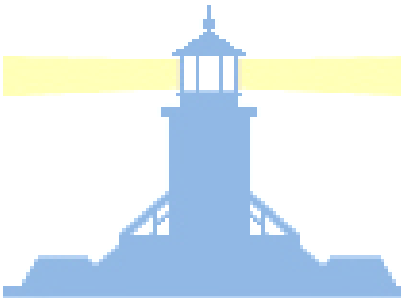
Roles vs. Responsibilities

 Argentine Payables	FND_RESP JL ARGENTINE_PAYABLES STANDARD	Latin America Localizations	✓			
 Argentine Receivables	FND_RESP JL ARGENTINE_RECEIVABLES STANDARD	Latin America Localizations	✓			
 Asset Inquiry	FND_RESP OFA FA_WEB_ASSET_INQUIRY STANDARD	Assets				
 Asset Inquiry Vision Belgium	FND_RESP OFA FA_WEB_ASSET_INQUIRY_BEL STANDARD	Assets	✓			
 Asset Inquiry Vision France	FND_RESP OFA FA_WEB_ASSET_INQUIRY_FR STANDARD	Assets	✓			
 Asset Inquiry Vision Germany	FND_RESP OFA FA_WEB_ASSET_INQUIRY_DE STANDARD	Assets	✓			
Next 151 - 165 of 2001						
 Security Administration						
 Approvals Management Administrator	UMX AME_APP_ADMIN	Human Resources				
 Approvals Management Business Analyst	UMX AME_BUS_ANALYST	Human Resources	✓			

Responsibilities begin with FND_RESP

Roles begin with UMX

User Management objects belong to FND schema



Seeded Security Administration Roles

[-] Security Administration					
[+] Approvals Management Administrator	UMX AME_APP_ADMIN	Human Resources	✓	✎	+
[+] Approvals Management Business Analyst	UMX AME_BUS_ANALYST	Human Resources	✓	✎	+
[+] Approvals Management Process Owner	UMX AME_BUS_PROCESS_OWNER	Human Resources	✓	✎	+
[+] Approvals Management System Administrator	UMX AME_TTYPE_ADMIN	Human Resources	✓	✎	+
[+] Approvals Management System Viewer	UMX AME_ADM_VIEWER	Human Resources	✓	✎	+
[+] Customer Administrator	UMX UMX_EXT_ADMIN	Application Object Library		✎	+
Manage Proxies	UMX UMX_MANAGE_PROXIES	Application Object Library	✓	✎	+
[+] Partner Administrator	UMX UMX_PARTNER_ADMIN	Application Object Library		✎	+
[+] Pirate Administrator	UMX UMX_PIRATE_ADMIN	Application Object Library	✓	✎	+
[+] Security Administrator	UMX SECURITY_ADMIN	Application Object Library		✎	+
[+] iReceivables Customer Administrator	UMX ARI_CUST_ADMIN	Receivables	✓	✎	+
iSetup Super User	UMX AZ_SUPER_USER	Application Implementation	✓	✎	+

Security Administrator can manage all users and assign/revoke roles

Customer Administrators manage in their own organization

Partner Administrators manage in their own and partner organizations





New Administrator Role Creation

ORACLE User Management Home Logout Preferences Help Diagnostics

User Management | **Roles & Role Inheritance** | Role Categories | Registration Processes

User Management: Roles & Role Inheritance >

Update Role : Pirate Administrator

* Indicates required field

* Category: Security Administration
Role Code: IMXUIMX PIRATE ADMIN
* Application: Application Object Library
From: 09-Aug-2007
(example: 25-Jul-2007)
To:

* **Pirate Administrator**
Description: Represents external pirates that manage user accounts and access for pirates in their own as well as any partner organizations.

Permissions

Name	Set	Object	Data Context Type	Access Policy	Last Update	Duplicate	Update	Delete
No results found.								

- Different administrator roles can be created to service different TCA party types (i.e. partners, customers, suppliers and even PIRATES!)





System Administration Security Wizards

- Two Security Wizards are packaged with Release 12 which provide breadcrumb setup processes
- MetaLink Doc. ID: 401463.1 suggests that more products will deliver security wizards in future patch releases

User Management : Security Administration Setup

ORACLE User Management Home Logout Preferences Help Diagnostics

User Management: Roles & Role Inheritance | Current Role : Pirate Administrator >

Security Wizards

Name	Description	Run Wizard
CE UMX Security wizard		
User Management : Security Administration Setup	Function for UMX security administration setup wizard	



Security Administration Wizard

ORACLE User Management

Home Logout Preferences Help Diagnostics

User Management

Users | Roles & Role Inheritance | Role Categories | Registration Processes

User Management: Roles & Role Inheritance >

Update Role : Pirate Administrator

* Indicates required field

Object	Data Context Type	Access Policy
User Management Person	Instance Set	People in Partner Organization
User Management Organization	Instance Set	View Partner Organizations
User Management Role	Instance	UMX UMX_PIRATE_ADMIN

Permissions

Create Grant

Name	Set	Object	Data Context Type	Access Policy	Last Update	Duplicate	Update	Delete
User Administration privileges	Basic User Administration Privileges	User Management Person	Instance Set	People in Partner Organizations	09-Aug-2007			
Organization Administration privileges	Organization Administration Privileges	User Management Organization	Instance Set	View Partner Organizations	09-Aug-2007			
Role Administration privileges	Assign / Revoke Role	User Management Role	Instance	UMX UMX_PIRATE_ADMIN	09-Aug-2007			

Cancel Security Wizards Save Apply

User Management Home Logout Preferences Help Diagnostics

About this Page Privacy Statement

Copyright (c) 2006, Oracle. All rights reserved.

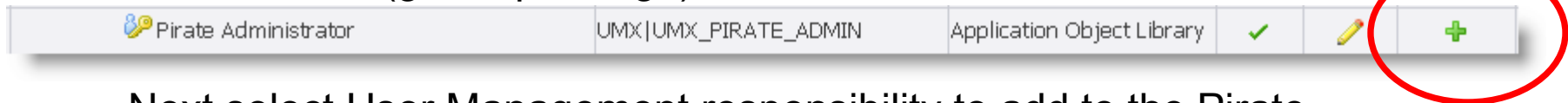
- Security Administration Wizard adds Data Security Policies
- Data Security Policies restrict actions that administrators can perform
- Data Security Policies also indicate which TCA parties and organizations can be administered





Pirate Administration Setup

- Next step is to add a navigable responsibility for User Management – click on Add Node (green plus sign)



- Next select User Management responsibility to add to the Pirate Administration role

A screenshot of the Oracle User Management web interface. The page title is 'ORACLE User Management'. The navigation menu includes 'User Management', 'Users', 'Roles & Role Inheritance', 'Role Categories', and 'Registration Processes'. The main heading is 'Define Role Inheritance Hierarchy: Search and Select Roles'. Below this is a search form with fields for 'Category', 'Name' (containing 'User management'), 'Code', and 'Application'. A 'Go' button is present. Below the search form is a table with columns: 'Select', 'Quick Select', 'Role', 'Code', 'Application', and 'Active'. The table contains one row for 'User Management' with code 'FND_RESP|FND|UMX|STANDARD' and application 'Application Object Library'. A red circle highlights the search form and the table. On the right side, there is a 'Legend' section with icons for 'Category', 'Role', 'Responsibility', 'All Users (Everyone)', and 'Externally Managed Group'. At the bottom right, there are 'Cancel' and 'Select' buttons.

ORACLE User Management

Home Logout Preferences Help Diagnostics

User Management

Users Roles & Role Inheritance Role Categories Registration Processes

Define Role Inheritance Hierarchy: Search and Select Roles

The role you select from the hierarchy will be inherited by everyone assigned the **Pirate Administrator** role.

Search

Category [dropdown]

Name

Code

Application

Go

Select	Quick Select	Role	Code	Application	Active
<input type="radio"/>		User Management	FND_RESP FND UMX STANDARD	Application Object Library	✓

Legend

- Category
- Role
- Responsibility
- All Users (Everyone)
- Externally Managed Group

Cancel Select

Cancel Select



Pirate Administration Setup

- Last step is to create grant for User Management Menu

ORACLE User Management Home Logout Preferences Help Diagnostics

User Management | **Roles & Role Inheritance** | Role Categories | Registration Processes

User Management: Roles & Role Inheritance > Update Role : Pirate Administrator >

View Grant: UMX Menu Delete Update

Name **UMX Menu**
Description **UMX Menu**
Effective From **13-Aug-2007**
Effective To

Security Context

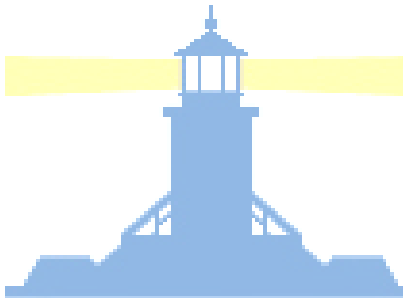
Grantee Type **Group Of Users**
Grantee **Pirate Administrator**
Operating Unit
Responsibility

Set

Name **User Maintenance UI's**
Code **UMX_USER_ADMIN_UI_PERMS**
Description **Gives access to the User Maintenance UI's. Must be granted to all User Administrator Roles.**

[Return to Grants](#) Delete Update





Pirate Administration Setup

Pirate Administrator	UMX UMX_PIRATE_ADMIN	Application Object Library
User Management	FND_RESP FND UMX STANDARD	Application Object Library

Indicates required field

Cancel | Reset Password | Save | Apply

Prefix: * User Name: jsparrow

First Name: Jack Email: Status: Active

Middle Name: Last Name: Sparrow

Quick Tips
Personal information originates from the HR system and cannot be updated here.

Pirate Administrator	Represents external pirates that manage user accounts and access for pirates in their own as well as any partner organizations.	Assign
Customer Administrator	Represents external people that manage user accounts / access for people in their own organization (defined as organization parties).	Assign
User Management	User Management	Assign

+ Show Pirate Administrator Represents external pirates that manage user accounts and access for pirates in their own as well as any partner organizations. Assigned

+ Show Customer Administrator Represents external people that manage user accounts / access for people in their own organization (defined as organization parties). Assigned

+ Show User Management User Management Assigned

Cancel | Reset Password | Save | Apply

- New Pirate Administration role now has wheels!
- Jack Sparrow can now administer other pirates through User Management





Jack Sparrow – Pirate Administrator

User Name Organization **Business World**
Email Role
Last Name
First Name

Maintain User Accounts
• Register new people, create/disable user accounts, and reset passwords.
 Control Access
• Grant access to different parts of the system by assigning/revoking roles.

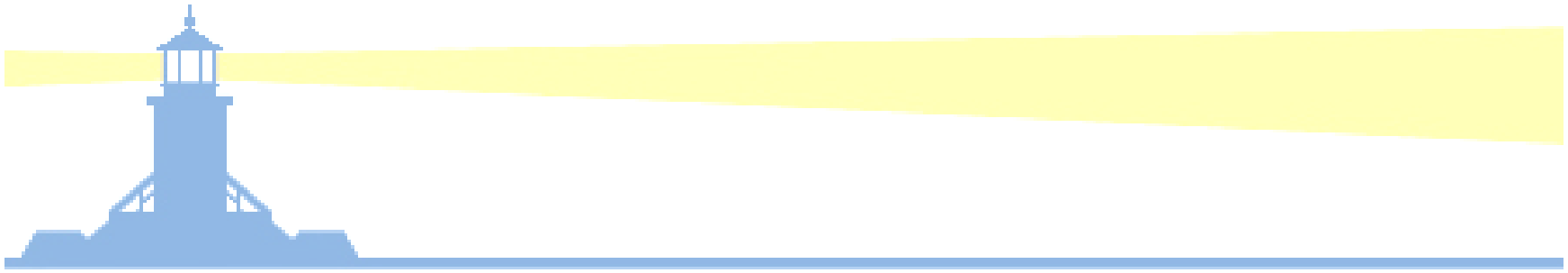
Register	<input type="text"/>	<input type="button" value="Go"/>	Previous 10	31-40	Next 10
Last Name	Sparrow	Jack	jsparrow	Active	<input type="button" value="Edit"/>
Smith	Swann	Elizabeth		Not Created	<input type="button" value="Edit"/>
Sparrow	Jack		jsparrow	Active	<input type="button" value="Edit"/>
Stein	Swann	Elizabeth		Not Created	<input type="button" value="Edit"/>
Stewart	Swann	Elizabeth		Not Created	<input type="button" value="Edit"/>
Tuppe	Turner	Will		Not Created	<input type="button" value="Edit"/>
Turaki	Turner	Will		Not Created	<input type="button" value="Edit"/>
Turner	Will			Not Created	<input type="button" value="Edit"/>
Verdi	Fabrizio		bworldit	Active	<input type="button" value="Edit"/>
Wang	Robert	rwang@bw.com	rwang	Active	<input type="button" value="Edit"/>

[Previous 10](#) 31-40 [Next 10](#)

User Management Home Logout Preferences Help Diagnostics

- Now login as Jack Sparrow and only users in the pirate organization can be managed





Manage Proxies

"Manage Proxies" Role

Delegating User must have the "Manage Proxies" role assigned to them

"Manage Proxies" role provisions the "Switch User" and "Return to Self" permission sets

User Management

Users | Roles & Role Inheritance | Role Categories | Registration Processes

User Management: Users >

Update User: ckennedy

* Indicates required field

Prefix: Kennedy
First Name: Chuck
Middle Name:
Last Name: Kennedy
Suffix:
Active:
Active To: 13-Apr-2007
(example: 29-Jan-2008)

Buttons: Cancel, Reset Password, Save, Apply

Quick Tips
Personal information originates from the HR system and cannot be updated here

Roles | Contact Information

Changes can only be made for roles you have been granted the privileges.

Assign Roles

Details	Role	Description	Status	Remove
Show	SB_CK_SPECIFIC_LE_VISION_JAPAN	SB_CK_SPECIFIC_LE_VISION_JAPAN	Assigned	
Show	Security Administrator	Security Administrators manage all user accounts in the system, and can assign / revoke all roles. Security Administrators also manage system accounts (such as GUEST), that are not tied to a person.	Assigned	
Show	Manage Proxies	Grant other users the right to access your user account, without sharing your password.	Assigned	





Manage Proxies

Under Preferences off the Home Page – find “Manage Proxies” on the left side

ORACLE User Management

Home Logout Preferences Help Personalize Page Diagnostics

User Management

- General
- Display
- Preferences
- Access Requests
- Manage Proxies**

General Preferences

Cancel Reset to Default Apply

Languages

Current Session Language American English ⓘ

Default Application Language American English ⓘ

Accessibility

Accessibility Features None ⓘ

Regional

Territory United States ▼

Under Preferences find "Manage Proxies"



Add Proxy User

- “Add People” button allows the delegating user to select their proxy user or users

ORACLE® User Management

Home Logout Preferences Personalize Page Diagnostics

User Management

Manage Proxies: Manage Proxies >

Manage Proxies

Manage the people that can access your account and act on your behalf.

Cancel! Apply

General

- Display Preferences
- Access Req
- Manage Proxies

Add People Run Proxy Report

Details	Last Name	First Name	User Name	Start Date	Date
+ Show	Sparrow	Jack	JSPARROW	29-Jan-2008 10:25:06	

Cancel! Apply

JSPARROW is now proxy for ckennedy



Proxy User Login

- Now logged in at JSPARROW which is the proxy user for CKENNEDY
- Select “Switch User”

The screenshot shows the Oracle E-Business Suite interface. At the top left, the text "ORACLE® E-Business Suite" is displayed. On the right side of the top navigation bar, there are links for "Diagnostics", "Logout", "Preferences", "Help", "Personalize Page", and "Switch User". The "Switch User" link is highlighted with a red rectangular box. Below the navigation bar, a status bar indicates "Logged In As JSPARROW", also highlighted with a red rectangular box. The main content area is divided into two sections: "Navigator" and "Favorites". The "Navigator" section contains a "Personalize" button and a link to "User Management" with the text "Please select a responsibility." below it. The "Favorites" section contains a "Personalize" button and a message: "You have not selected any favorites. Please use the 'Personalize' button to set up your favorites."



Switch User

- Select "Switch" to change from JSPARROW to CKENNEDY

ORACLE® E-Business Suite

Diagnostics Home Logout Preferences Personalize Page

Logged In As JSPARROW

Switch User

Select a user and act as their proxy

Switch	Last Name ▲	First Name	User Name	Job Title	Phone	Email
	Kennedy	Chuck	CKENNEDY			



Proxy User Now Is Delegated User

- JSPARROW is now masquerading as CKENNEDY with all of CKENNEDY roles and responsibilities
- Does not need to know CKENNEDY password
- When done with proxy duties – hit “Return to Self”

The screenshot shows the Oracle E-Business Suite interface. At the top, the Oracle logo and 'E-Business Suite' are visible. The top navigation bar includes links for 'Logout', 'Preferences', 'Help', 'Personalize Page', and 'Return to Self'. A red box highlights the user information: 'Logged In As JSPARROW Proxy For CKENNEDY'. A callout bubble points to the 'Return to Self' link, stating: 'When Jack Sparrow is done with proxy duties - he hits "Return to Self"'. Below the navigation bar is the 'Navigator' section with a list of responsibilities and a 'Personalize' button. A 'Favorites' section is also visible with a 'Personalize' button and a message: 'You have not selected any favorites. Please use the "Personalize" button to set up your favorites.' A second callout bubble points to the 'Personalize' button in the Favorites section, stating: 'Jack Sparrow is now logged in as CKENNEDY'.





Proxy Report

- Must run the “Page Access Tracking Data Migration” concurrent program to make proxy accesses available to the Proxy Report
- Go to “Manage Proxies” and select “Run Proxy Report”

ORACLE®

Close Window Preferences Personalize Page Diagnostics

User Management

Manage Proxies: Manage Proxies >

Proxy Report

Following are the pages that this proxy accessed

User Name

Effective From
(example: 29-Jan-2008)

Responsibility

To
(example: 29-Jan-2008)

Actions taken by proxy JSPARROW when using CKENNEDY's roles and responsibilities

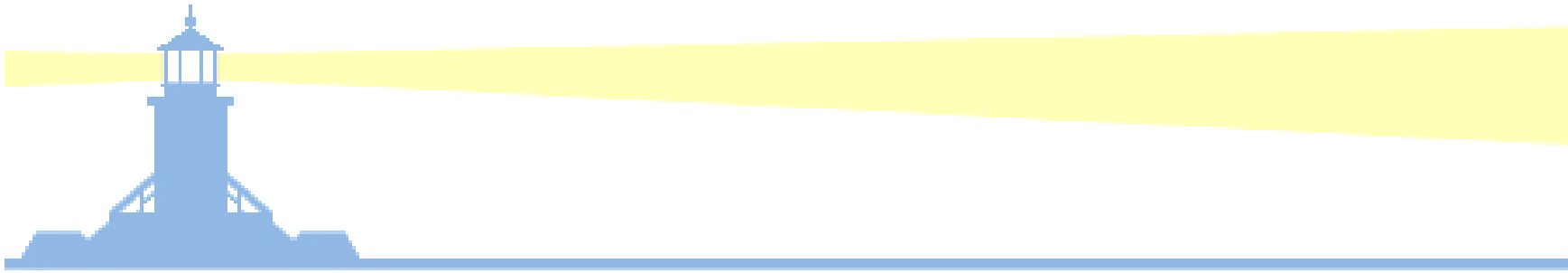
User Name	Responsibility	Action	Date
JSPARROW	System Administrator	LOGIN	29-Jan-2008 11:06:56
JSPARROW	System Administrator	LOGIN	29-Jan-2008 12:59:23
JSPARROW	System Administrator	LOGOUT	29-Jan-2008 11:08:00
JSPARROW	System Administrator	LOGOUT	29-Jan-2008 13:02:56
JSPARROW	System Administrator	RESP_CHANGE	29-Jan-2008 11:07:26
JSPARROW	System Administrator	RESP_CHANGE	29-Jan-2008 12:59:53





Identifying Proxy Users

- Run the following SQL to find those users who have the “Manage Proxies” role assigned to them
- ```
select * from wf_user_role_assignments_v
where role_name = 'UMX|UMX_MANAGE_PROXIES'
and start_date <= sysdate
and (end_date is null OR end_date >= sysdate)
```
- Important to understand proxy user relationships from a controls perspective



# Pervasiveness of UMX in Release 12





# Release 12 Role Groups

Role Inheritance Hierarchy

Create Role


| Focus | Name                                        | Code | Application | Active | Update | Add Node | Remove Node |
|-------|---------------------------------------------|------|-------------|--------|--------|----------|-------------|
|       | [-] All Roles, Responsibilities, and Groups |      |             |        |        |          |             |
| +     | [-] Roles & Re                              |      |             |        |        |          |             |
| +     | [-] Training                                |      |             |        |        |          |             |
| +     | [-] Miscella                                |      |             |        |        |          |             |
| +     | [-] Security                                |      |             |        |        |          |             |
| +     | [-] Informa                                 |      |             |        |        |          |             |
| +     | [-] Territor                                |      |             |        |        |          |             |
| +     | [-] Territor                                |      |             |        |        |          |             |
| +     | [-] Release                                 |      |             |        |        |          |             |
| +     | [-] Solution                                |      |             |        |        |          |             |
| +     | [-] Groups fro                              |      |             |        |        |          |             |

- + Training
- + Miscellaneous
- + Security Administration
- + Information Technology
- + Territory Management Task Roles
- + Territory Management Job Roles
- + Release 12 Core Team
- + Solution Beacon
- + Groups from other Source Systems

Create Role

- View the seeded role groups by logging into UMX and going to Roles and Role Inheritance
- Expand the role groups to see the underlying E-Business Suite Applications



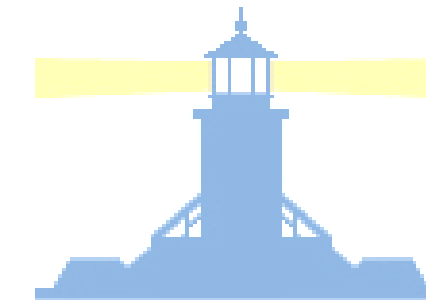


# Release 12 Role Groups

| UMX/RBAC Role Groups             | E-Business Suite Application Ownership                |
|----------------------------------|-------------------------------------------------------|
| Training                         | Learning Management                                   |
| Miscellaneous                    | All Responsibilities                                  |
| Security Administration          | UMX/RBAC Security Administration                      |
| Information Technology           | Integration Repository (IREP)                         |
| Territory Management Task Roles  | CRM – Territory Management                            |
| Territory Management Job Roles   | CRM – Territory Management                            |
| Groups from other Source Systems | Trading Community Architecture and HR Roles/Positions |

- Underlying E-Business Suite Applications
- Doesn't provide the complete picture – need to look at Permission Sets

# Release 12 Permission Sets



|                                         |                                              |                                  |
|-----------------------------------------|----------------------------------------------|----------------------------------|
| Complex Maintenance Repair and Overhaul | Internal Controls Manager                    | Self Service Receivables         |
| Applications BIS                        | Balanced Scorecard                           | Cash Management                  |
| Incentive Compensation                  | Depot Repair                                 | Service                          |
| <u>Configurator</u>                     | <u>Document Management and Collaboration</u> | Enterprise Asset Management      |
| Advanced Product Catalog                | Engineering                                  | Financial Intelligence           |
| Application Object Library              | Project Portfolio Analysis                   | Financials Common Modules        |
| Scripting                               | Collections                                  | Grants Proposal                  |
| Customers Online                        | Inventory                                    | <u>iRecruitment</u>              |
| CRM Foundation                          | Project Contracts                            | CRM - Sales Territory Management |
| Learning Management                     | Project Intelligence                         | Purchasing Intelligence          |
| Sourcing                                | Purchasing                                   | Advanced Pricing                 |
| UMX Security Administration             | Workflow                                     | Work in Process                  |
| Approvals Management Engine (AME)       |                                              |                                  |

```
select * from
apps.fnd_menus a,
apps.fnd_menus_tl b
where a.type =
'SECURITY'
and a.menu_id =
b.menu_id
order by a.menu_name;
```

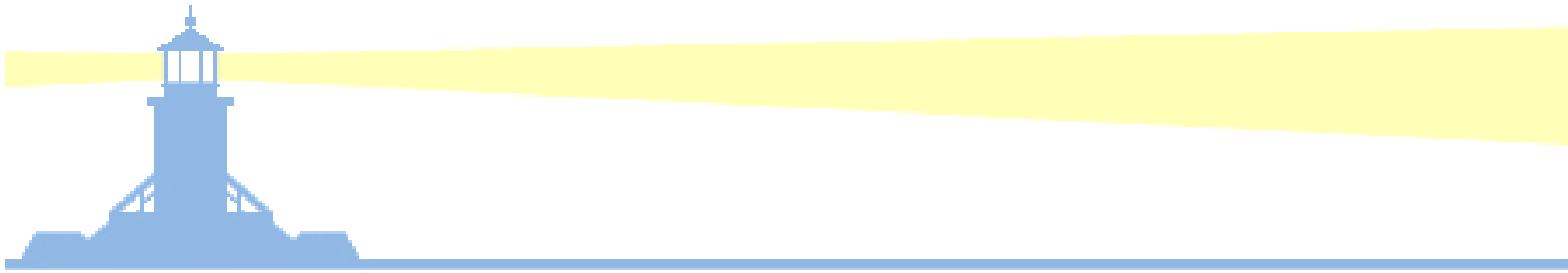




# Applications To Audit

| E-Business Suite Application      | UMX/RBAC Access |
|-----------------------------------|-----------------|
| Approvals Management Engine (AME) | All accesses    |
| Workflow                          | All accesses    |
| UMX Security Administration       | All accesses    |
| Cash Management                   | All accesses    |
| Application Object Library        | All accesses    |
| Trading Community Architecture    | All accesses    |

- Applications where all their UMX roles should be examined .
- These roles that can be provisioned within these applications can have high impact across the Release 12 E-Business Suite



# SYSADMIN May Be Old....



# SYSADMIN Userid

- Upgrades require SYSADMIN to be active (point in time, planned activity)
- The Release 11.0 to Release 11i Category 3 steps require the SYSADMIN user to be active
- The Release 11.0 to Release 12 upgrade path involves upgrading first to 11.5.10.2, which requires the same Category 3 step mentioned above
- In a Portal/SSO environment, SYSADMIN is required as the backup method to perform the administration tasks and troubleshooting if something happens to the Single Sign-on (SSO) infrastructure and it fails to work as designed
- Over 350 specific lines of E-Business Suite Release 12 code reference SYSADMIN (select \* from sys.dba\_source where text like '%SYSADMIN%';)



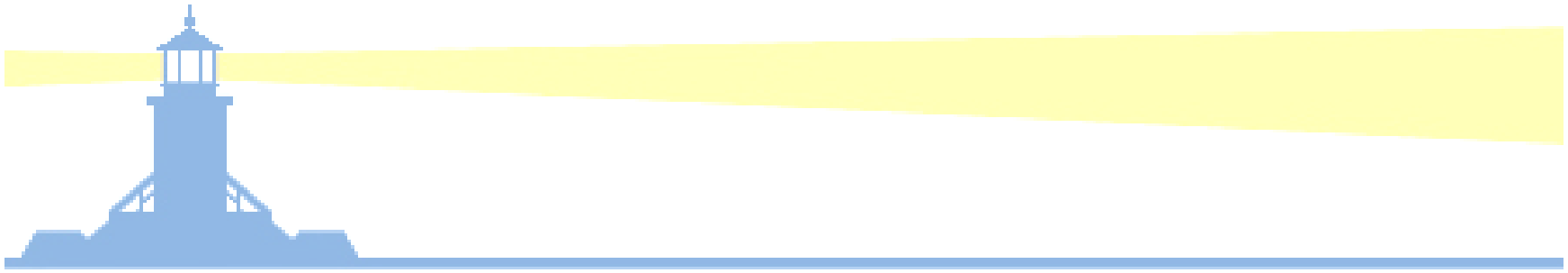
# SYSADMIN Userid

- The following system level profile options are defaulted to SYSADMIN at implementation:
  - AP: Invoice Approval Workflow User
  - GMI: Workflow Default Item Approver
  - OKC: Change Request Approver
  - OKC: Contract Approver
  - OKL: Credit Analyst
  - OKL: Funding Approver
  - OM: Notification Approver



# SYSADMIN Userid

- Unless changed, Oracle Workflow will fail because SYSADMIN is the default workflow administrator and is used to communicate user security events, violations and exceptions (see MetaLink Doc. IDs: 259319.1 and 333656.1)
- Upon implementation, SYSADMIN is the initial and original grantor of UMX Security Administration (point-in-time, planned activity)
- SYSADMIN is the default userid used to startup the concurrent managers. Alternatively, a custom script could be developed to use a different userid that has the associated System Administrator responsibility
- Historically, many patches have required SYSADMIN to be active – patch analysis should check for this and, if required, SYSADMIN could be activated (point-in-time, planned activity)



# Sensitive Data





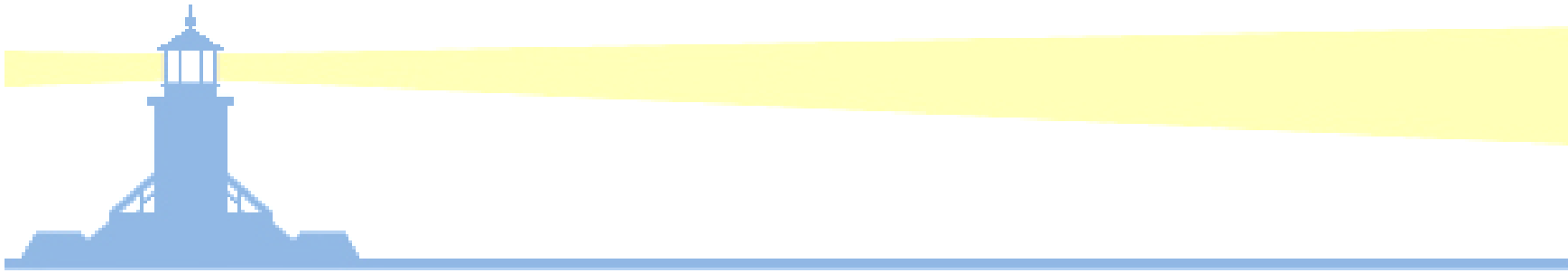
# Sensitive Data in Production

- Personalizations
- Database roles and privileges
- Direct database restrictions
- Release 12 Payments and Cash Management Masking and Encryption
- Above all else – IDENTIFY sensitive data elements
- Know where sensitive data elements come to rest



# Sensitive Data in Non-Production

- Additionally for Non-Production Environments....
- Oracle Applications Management Pack includes scrambling as part of clone process
- Obfuscate or destroy sensitive data elements
- Search and destroy package available from <http://www.solutionbeacon.com/security>
- Above all else – IDENTIFY sensitive data elements



# Conclusion and Recommendations



# Recommendations

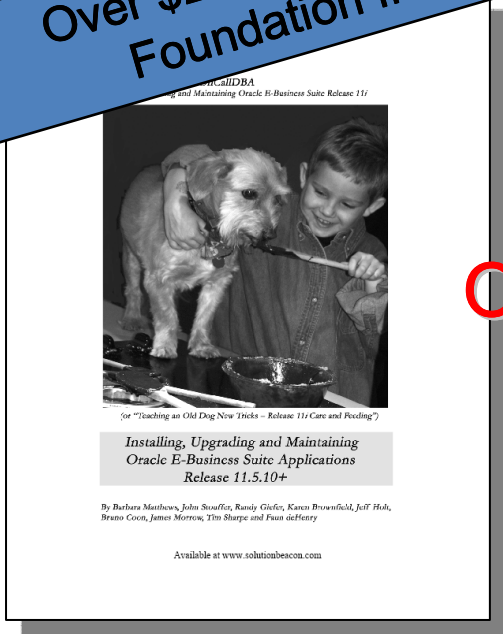
- Check on the UMX roles for the high-impact applications mentioned previously
- Create an alert to notify when SYSADMIN is used
- Change the SYSADMIN password frequently
- Obfuscate your sensitive data in non-production environments
- Check database roles and privileges in production
- Consider restricting direct connections to the database



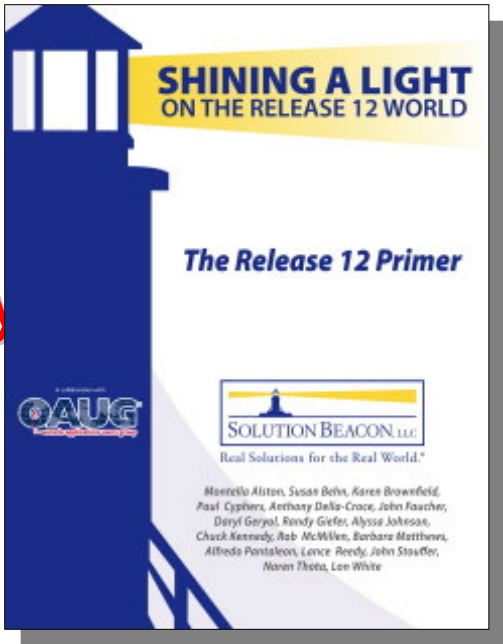
Over \$24,800 donated to the Solution Beacon Foundation from the sale of our books!

# Got Oracle? Get the Books!

Order Your Copy Today



Installing, Upgrading and Maintaining Oracle E-Business Suite Applications 11.5.10.2+



The Release 12 Primer – Shining a Light on the Release 12 World

Available at [www.solutionbeacon.com](http://www.solutionbeacon.com)





# Oracle Applications Users Group (OAUG)

- THE world's largest knowledgebase for Oracle Applications users
- Networking opportunities with over 118,000 members worldwide
- Access to over 50,000 white papers in the online OAUG Conference Paper Database
- FREE online training every Tuesday, Wednesday and Thursday for OAUG members





# Questions and Answers

Thank You!

Chuck Kennedy

[ckennedy@solutionbeacon.com](mailto:ckennedy@solutionbeacon.com)

Susan Behn

[sbehn@solutionbeacon.com](mailto:sbehn@solutionbeacon.com)

Brian Bent

[bbent@solutionbeacon.com](mailto:bbent@solutionbeacon.com)

[www.solutionbeacon.com](http://www.solutionbeacon.com)

*Real Solutions for the Real World<sup>®</sup>*



Copyright 2008 Solution Beacon, LLC All Rights Reserved Any other commercial product names herein are trademark, registered trademarks or service marks of their respective owners.

