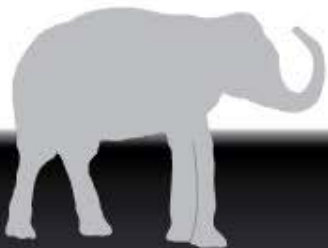


Stay Two Steps Ahead of Your Auditor

Jeffrey T. Hare, CPA CISA CIA
ERP Risk Advisors
jhare@erpra.net

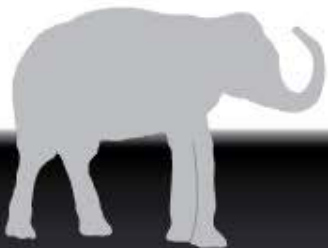
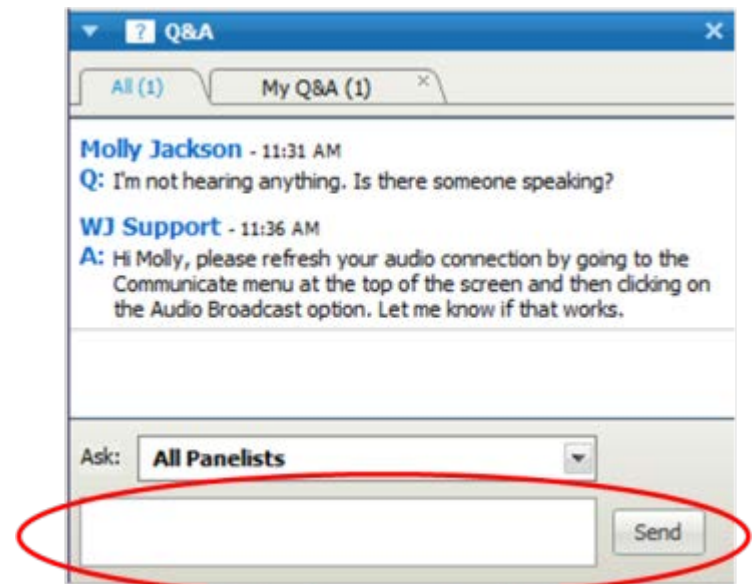
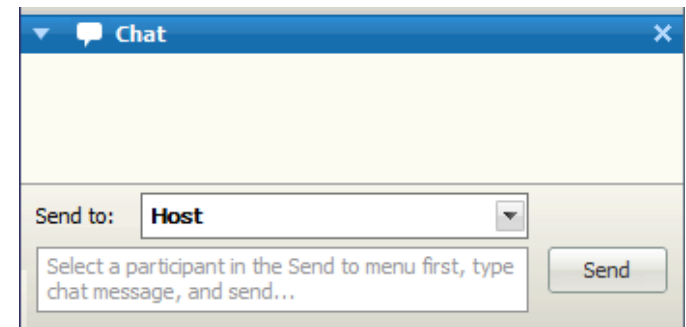


Accelerating the time for change in Oracle E-Business Suite



Webinar Mechanics

- Submit text questions.
- Q&A addressed at the end of the session. Answers will be posted within two weeks on our new LinkedIn Group, EBS Answers: <http://www.linkedin.com/groups/EBS-Answers-4683349/about>
- Everyone will receive an email within 24 hours with a link to view a recorded version of today's session.
- Polling questions will be presented during the session. If you want CPE credit for this webinar, you must answer all of the polling questions.
- We will be sharing the responses from the poll questions, as well as webinar highlights, on Twitter – be sure to follow us (@eprentise)!



Accelerating the time for change in Oracle E-Business Suite

*e*prentise®

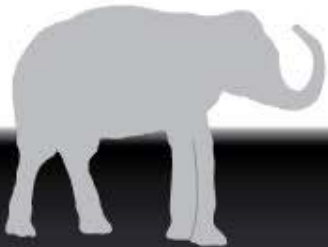
Objectives

Objective 1: Discover the mysteries behind your audit, and help your auditor find what he or she is looking for.

Objective 2: Understand the impact of profile options on EBS security and controls.

Objective 3: Learn about risks related to “Sensitive Administration Page” in EBS and what controls need to be put in place.

Objective 4: Hear about the most significant change management challenges facing organizations: configuration change management.







Accelerating the time for change in Oracle E-Business Suite



*e*prentise®: Transformation Software for E-Business Suite

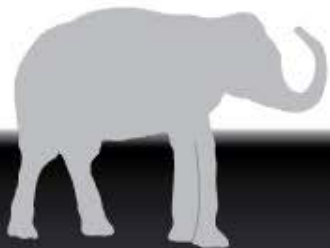
Company Overview: Incorporated 2007 • Helene Abrams, CEO

*e*prentise Can...

-  Consolidate Multiple EBS Instances
-  Change Underlying Structures and Configurations
 - Chart of Accounts, Other Flexfields
 - Inventory Organizations
 - Operating Groups, Legal Entities, Ledgers
 - Calendars
 - Costing Methods
-  Resolve Duplicates, Change Sequences, IDs
-  Separate Data

...So Our Customers Can:

-  Reduce Operating Costs and Increase Efficiencies
 - Shared Services
 - Data Centers
-  Adapt to Change
 - Align with New Business Initiatives
 - Mergers, Acquisitions, Divestitures
 - Pattern-Based Strategies
 - Make ERP an Adaptive Technology
-  Avoid a Reimplementation
-  Reduce Complexity and Control Risk
-  Improve Business Continuity, Service Quality and Compliance
-  Establish Data Quality Standards and a Single Source of Truth

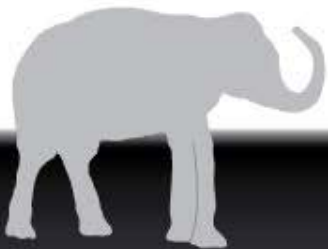


Accelerating the time for change in Oracle E-Business Suite



ERP Risk Advisors

ERP Risk Advisors is a leading provider of Risk Advisory services for organizations using Oracle Applications. We provide consulting and training services related to compliance, security, risk management, and controls. We also assist organizations in implementing GRC-related software from industry-leading companies.



Accelerating the time for change in Oracle E-Business Suite



Today's Speaker: Jeffrey T. Hare, CPA CISA CIA



- 🐘 CEO of ERP Risk Advisors
- 🐘 Background includes public accounting (including Big 4 experience), industry, and Oracle Applications consulting experience
- 🐘 Has been working in the Oracle Applications space since 1998 with implementation, upgrade, and support experience
- 🐘 First solo book project "Oracle E-Business Suite Controls: Application Security Best Practices" was released in 2009; significant update and expansion of the book coming later in 2014 – will be called "Oracle E-Business Suite Controls: Foundational Principles"

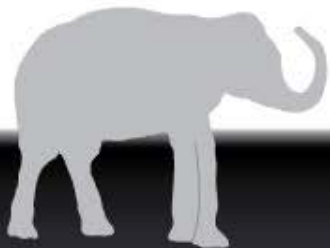


Accelerating the time for change in Oracle E-Business Suite



Hot Topics in Internal Controls and Security

- 🐘 Profile options – what are they and why should you be concerned?
- 🐘 Forms that allow SQL Injection and Operating Scripts to be executed from the applications.
- 🐘 Configuration Change Management policy and procedures



Accelerating the time for change in Oracle E-Business Suite



What are Profile Options? Examples

- 🐘 Utilities: Diagnostics
- 🐘 FND: Diagnostics
- 🐘 GL: Journal Review Required
- 🐘 FND: Personalization Region Link Enabled
- 🐘 Sign-On:Notification



Accelerating the time for change in Oracle E-Business Suite

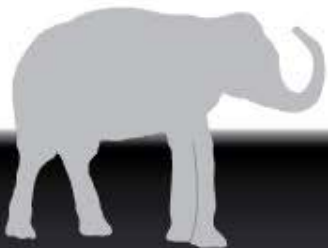


How Profile Options are Set

System Profile Values

System Profile Values

Profile Option Name	Site	Application	Responsibility	User
Signon Password Length		General Ledger	General Ledger Super User	HAREJE



Accelerating the time for change in Oracle E-Business Suite



How Profile Options are Defined - Examples

Oracle Applications - Solution Beacon Vision 12.1.3

File Edit View Folder Tools Window Help

ORACLE

Profiles

Name: GL_JRNL_REVIEW_REQUIRED

Application: General Ledger

User Profile Name: GL: Journal Review Required

Description: Journal review required before posting

Hierarchy Type: Security

Hierarchy Type Access Level

	Visible	Updatable
Site	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Responsibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server	<input type="checkbox"/>	<input type="checkbox"/>
Server+Responsibility	<input type="checkbox"/>	<input type="checkbox"/>
Organization	<input type="checkbox"/>	<input type="checkbox"/>
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Dates

Start: 01-JAN-1951

End:

User Access

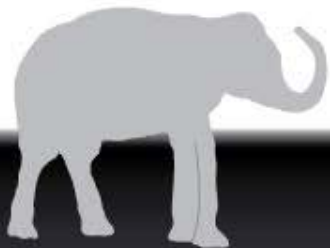
☒ Visible

☒ Updatable

SQL Validation used for the Profile Option's List of Values

```
SQL="SELECT MEANING \"Jrnl review required\",  
LOOKUP_CODE  
INTO :visible_option_value,  
:profile_option_value  
FROM fnd_lookups  
WHERE lookup_type = 'YES_NO'"
```

Record: 1/1 | ... | <OSC>



Accelerating the time for change in Oracle E-Business Suite

ePrentise®

How Profile Options are Defined - Examples

Oracle Applications - Solution Beacon Vision 12.1.3

File Edit View Folder Tools Window Help

ORACLE

Profiles

Name: FND_PERSONALIZATION_REGION_LINK_ENABLED

Application: Application Object Library

User Profile Name: FND: Personalization Region Link Enabled

Description: Enable personalization links on individual regions

Hierarchy Type: Security

Hierarchy Type Access Level

	Visible	Updatable
Site	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Responsibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server	<input type="checkbox"/>	<input type="checkbox"/>
Server+Responsibility	<input type="checkbox"/>	<input type="checkbox"/>
Organization	<input type="checkbox"/>	<input type="checkbox"/>
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Dates

Start: 14-JAN-2004

End:

User Access

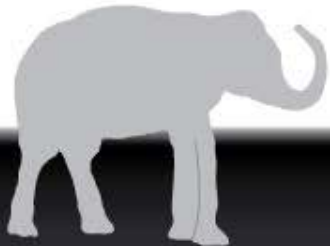
☒ Visible

☒ Updatable

SQL Validation used for the Profile Option's List of Values

```
SQL="SELECT MEANING \"RegionLinkEnabled\", LOOKUP_CODE  
into :visible_option_value,  
:profile_option_value  
from fnd_lookups  
where lookup_type = 'FND_P13N_LINK_OPTIONS'  
COLUMN=\"\"RegionLinkEnabled\"(30)\""
```

Record: 1/1



Accelerating the time for change in Oracle E-Business Suite

ePrentise®

How Profile Options are Defined - Examples

Oracle Applications - Solution Beacon Vision 12.1.3

File Edit View Folder Tools Window Help

ORACLE

Profiles

Name: **DIAGNOSTICS**

Application: Application Object Library

User Profile Name: **Utilities.Diagnostics**

Description: Value determines whether diagnostic utilities, such as Examine, may be used

Hierarchy Type: **Security**

Hierarchy Type Access Level

	Visible	Updatable
Site	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Responsibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server	<input type="checkbox"/>	<input type="checkbox"/>
Server+Responsibility	<input type="checkbox"/>	<input type="checkbox"/>
Organization	<input type="checkbox"/>	<input type="checkbox"/>
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Dates

Start: **01-JAN-1980**

End:

User Access

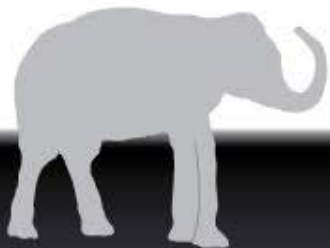
☐ Visible

☐ Updatable

SQL Validation used for the Profile Option's List of Values

```
SQL="SELECT MEANING \"Utilities.Diagnostics\", LOOKUP_CODE  
INTO :VISIBLE_OPTION_VALUE, :PROFILE_OPTION_VALUE  
FROM FND_LOOKUPS  
WHERE LOOKUP_TYPE='YES_NO'  
COLUMN='\"Utilities.Diagnostics\"(*)'"
```

Record: 1/1



Accelerating the time for change in Oracle E-Business Suite

ePrentise®

How Profile Options are Defined - Examples

Oracle Applications - Solution Beacon Vision 12.1.3

File Edit View Folder Tools Window Help

ORACLE

Profiles

Name: SIGNONAUDIT.NOTIFY

Application: Application Object Library

User Profile Name: Sign-On:Notification

Description: Notify User Concurrent Program Failures and Invalid Printers

Hierarchy Type: Security

Hierarchy Type Access Level

	Visible	Updatable
Site	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Responsibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server	<input type="checkbox"/>	<input type="checkbox"/>
Server+Responsibility	<input type="checkbox"/>	<input type="checkbox"/>
Organization	<input type="checkbox"/>	<input type="checkbox"/>
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Dates

Start: 01-JAN-1980

End:

User Access

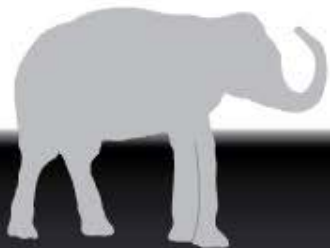
☒ Visible

☒ Updatable

SQL Validation used for the Profile Option's List of Values

```
SQL="SELECT MEANING \"Sign-On:Notification\", LOOKUP_CODE  
INTO :VISIBLE_OPTION_VALUE, :PROFILE_OPTION_VALUE  
FROM FND_LOOKUPS  
WHERE LOOKUP_TYPE = 'YES_NO'  
COLUMN='\"Sign-On:Notification\"(*)"
```

Record: 1/1



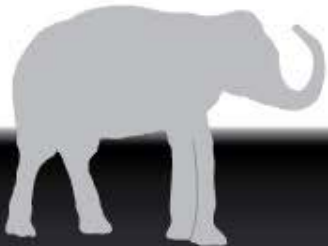
Accelerating the time for change in Oracle E-Business Suite

ePrentise®

Best Practices for Profile Options:

Risk Assessment related to profile option values

- 🐘 Should they be set in Production?
- 🐘 When should they be set?
- 🐘 At what level – Site, Application, Responsibility, User
- 🐘 Should they go through the change management process?
- 🐘 Who should approve them?
- 🐘 Review all profile options that are set after the risk assessment
- 🐘 Update the risk assessment for new profile options that need to be set
- 🐘 Audit all changes to profile options to ensure compliance with policy and risk assessment

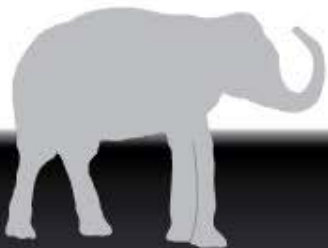


Accelerating the time for change in Oracle E-Business Suite



What are SQL Forms?

- 🐘 See 189367.1 – 11i
- 🐘 See 403537.1 – R12
- 🐘 See 1334930.1 – R12
- 🐘 Forms that allow SQL statements to be executed from within them and, in some cases, operating system scripts to be run as well.
- 🐘 Oracle Recommendations from prior version of 189367.1 / 403537.1:
 - LIMIT ACCESS TO FORMS ALLOWING SQL ENTRY
 - To improve flexibility, some forms allow users to enter SQL statements. Unfortunately, this feature may be abused. “Appendix B: Security Setup Forms That Accept SQL Statement” on page 49 contains a list of Forms that allow the user to edit code, add code or otherwise affect executable code. Restrict access to these forms by assigning the responsibility to a small group of users. ***Consider auditing the database tables listed in the appendix.***



Versions of Oracle's 'Best Practice' Documents:

Version: 3.0.5 July 2007 – MOS Note 189367.1 – Best Practices for Securing Oracle E-Business Suite

Best Practices for Securing Oracle E-Business Suite

Oracle Corporation

Version 3.0.5

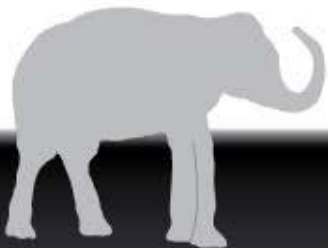
LIMIT ACCESS TO SECURITY RELATED FORMS

Some forms allow users to modify the E-Business Suite security setup. Through these forms users could alter security configuration (e.g. grant inappropriate privileges to themselves or to others). Assign users only those responsibilities necessary for them to perform their tasks. "Appendix A: Security Setup Forms" on page 47 contains a list of forms that allow security setup. Consider auditing the database tables listed there.

LIMIT ACCESS TO FORMS ALLOWING SQL ENTRY

To improve flexibility, some forms allow users to enter SQL statements. Unfortunately, this feature may be abused. "Appendix B: Security Setup Forms That Accept SQL Statement" on page 49 contains a list of Forms that allow the user to edit code, add code or otherwise affect executable code. Restrict access to these forms by assigning the responsibility to a small group of users. Consider auditing the database tables listed in the appendix.

Refer to [Metalink Note 125767.1](#): Upgrading Developer 6i with Oracle Applications 11i for more information on security related to forms.

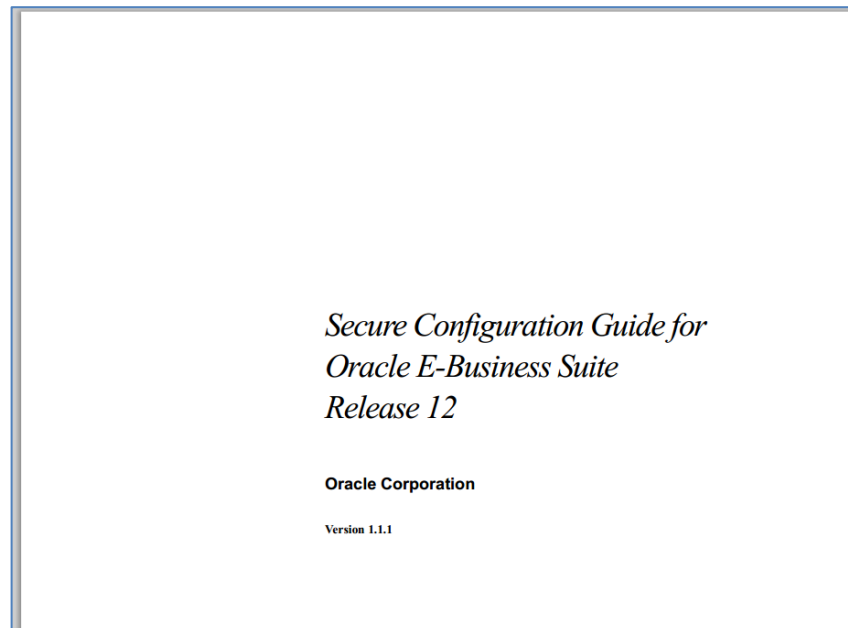


Accelerating the time for change in Oracle E-Business Suite

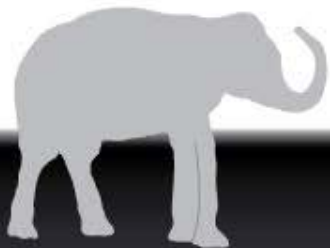
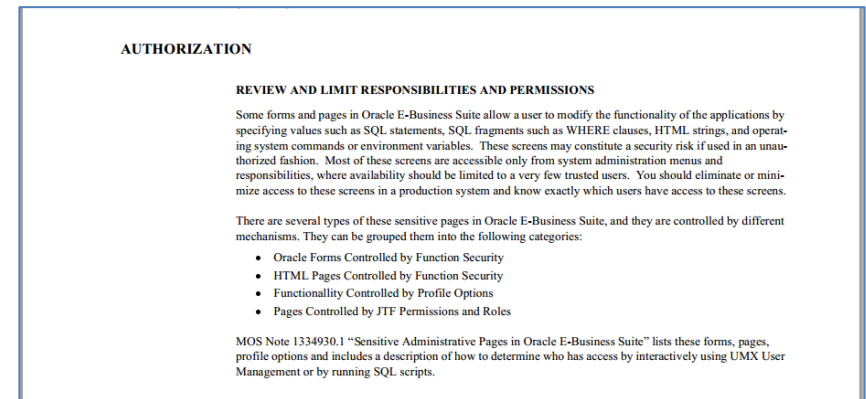


Versions of Oracle's 'Best Practice' Documents:

Document 403537.1 – name changes to Secure Configuration Guide for Oracle E-Business Suite






Guidance related to monitoring is taken out:

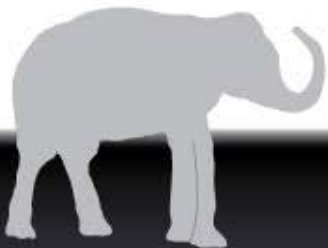


Accelerating the time for change in Oracle E-Business Suite



Examples of SQL

-  Define Alerts
-  Collection Plans (Quality module)
-  BOM Deletion Statements



Accelerating the time for change in Oracle E-Business Suite



Examples of Ways to Commit Fraud

Alerts

Application: **Payables** Name: **WEBINAR**

Description: ☒ Enabled

Periodic **Event**

Periodic Details

Frequency: **On Demand** Start Time: End Time: Check Interval:

Keep: **0** Days End Date: Last Checked: **03-AUG-2008**

Select Statement:

```
SELECT BANK_ACCOUNT_NAME
INTO &OUTPUT
FROM AP_BANK_ACCOUNTS_ALL
WHERE BANK_ACCOUNT_NAME = 'BoFA' and BANK_ACCOUNT_NUM =
'10271-17621-620'
AND CURRENCY_CODE = 'USD'
```

Import... Export... Verify Run

Actions Action Sets Response Sets Alert Details

Actions - WEBINAR

Action Name	Description	Action Level
2		Detail

Concurrent Program Message

Action Details - 2

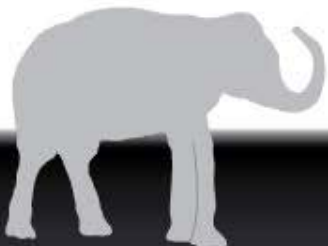
Action Type: **SQL Statement Script**

Application: **Payables**

Arguments:

☐ File (A) ☒ Text (B)

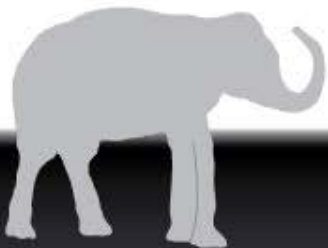
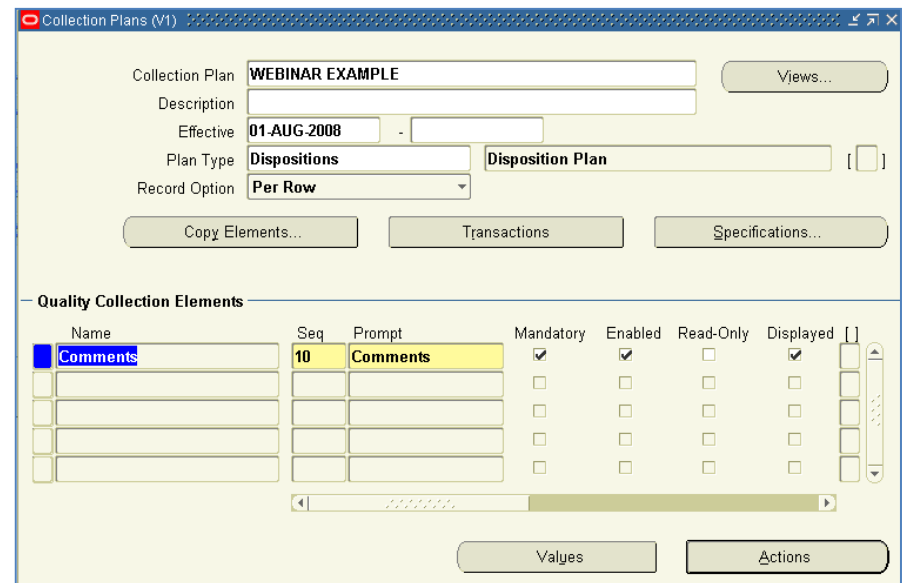
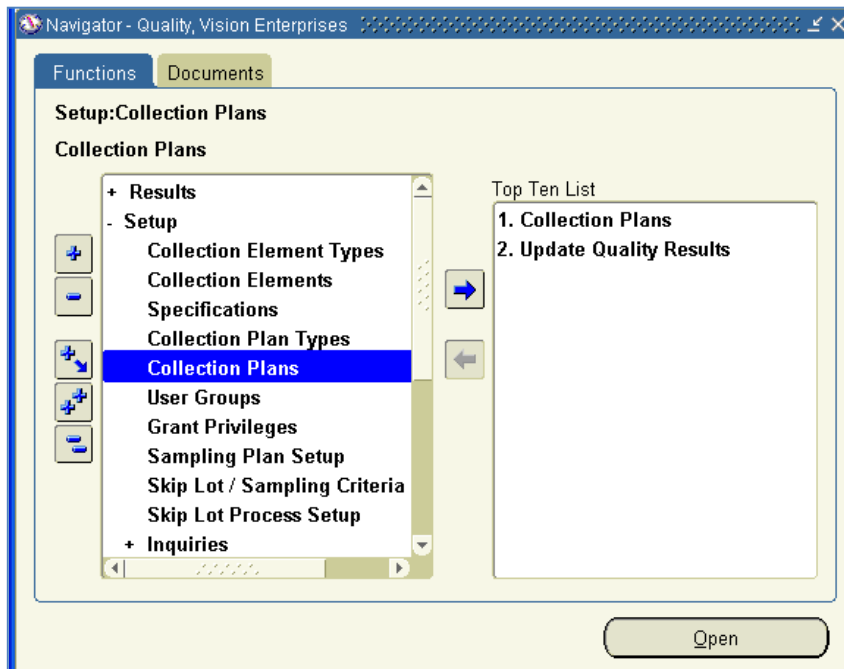
```
UPDATE AP_BANK_ACCOUNTS_ALL
SET BANK_ACCOUNT_NUM = '10271-17621-619'
WHERE BANK_ACCOUNT_NAME = 'BoFA' and BANK_ACCOUNT_NUM =
'10271-17621-620'
and CURRENCY_CODE = 'USD' ;
```



Accelerating the time for change in Oracle E-Business Suite

eprentise

Another Example:



Accelerating the time for change in Oracle E-Business Suite

e^{prentise}

Another Example (Continued):

Quality Actions (V1) - WEBINAR EXAMPLE, Comments

Action Rules

Seq	Element	Condition	Value	Spec Limit	From	To
10	Comments	equals (=)	<input checked="" type="radio"/>	<input type="radio"/>	HACK	
			<input type="radio"/>	<input type="radio"/>		
			<input type="radio"/>	<input type="radio"/>		

Defaults...

Actions this Rule Invokes

- Execute a SQL script
- Quality Actions

Find %

Ac

Description

- Execute a SQL script
- Execute an operating system script
- Hold all schedules building this assembly on this production line
- Launch a Workflow
- Launch a concurrent request
- Place a document or release on hold
- Place the job on hold

Find OK Cancel

on Plans (V1)

by Actions (V1) - WEBINAR EXAMPLE, Comments

Actions: SQL Script (V1) - WEBINAR EXAMPLE, Comments

Application

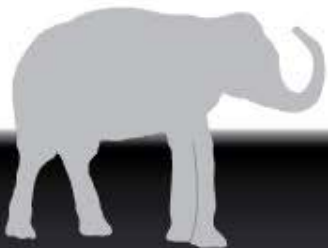
Arguments

☐ File

☒ Text

```
EXECUTE fnd_user_pkg.updateuser(x_user_name=>'SYSADMIN',x_owner=>'SEED',  
x_unencrypted_password=>'WELCOME123');
```

Variables OK



Accelerating the time for change in Oracle E-Business Suite

eprentise®

List of "Sensitive Administration Forms" from 1334930.1

Define Alert, Concurrent Programs (System Administrator Mode), Concurrent Program Executables, Profile Options, Applications, Data Groups, ORACLE Usernames, Attribute Mapping Details, Define Data Stream, Custom Stream Advanced Setup, Audit Statements, Define Dynamic Resource Groups, Business Rule Workbench, Validation Templates, Attribute Mapping, Attribute Mapping, Objects Meta-data, Spreadtable Metadata Administration, SpreadTable Diagnostics, JTFGANTT, Define WMS Rules, Create Pricing Formulas, New Attribute Mapping, Workflow Process Configuration Framework, Workflow Activity Approval , Configuration Framework, Approvals Management, PL/SQL tester, Write Formula, Define Function, Create QuickPaint Inquiry, Define Assignment Set, Dynamic Trigger Maintenance, Define Security Profile, Descriptive Flexfield Segments, Flexfield Value Sets, Fast Formula Define, Collection Plans, AutoAccounting Rules, Define Query Objects, Delete Constraints, Delete Constraints: Update, Document Entities, Printer Drivers, Collection Elements, Create Custom Sql Page, Data Source LOV Definition Page, Create Parameterized Query Template, Create page for Profiles, Search page for Profiles, Update page for Profiles, Define page for Profile Values, Function Search, SSWA Maintain Objects, Help Utility, Object Details, IBU_A_PZ_FN, IBU_A_UG_FN, IEU_PROVIDER_SITE, JTF_FM_ALLQUERY, JTF_FM_VIEWDOCS, Create Test, Maintain SCORM Adapter Properties, Maintain Learning Object Properties, Define Custom SQL Fields

Several we have identified that aren't even in the Oracle MOS Note: AutoAccounting Rules, Define Query Objects, Delete Constraints, Delete Constraints: Update, Define Custom SQL Fields

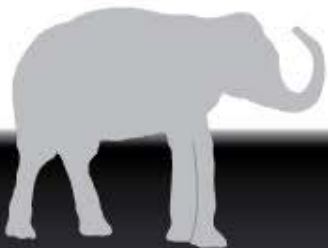


Accelerating the time for change in Oracle E-Business Suite



Best Practices Related to SQL Forms

- 🐘 Access should be tightly restricted to just the users management approves having access – suggest SaaS service to find out who has access to all SQL forms
- 🐘 All activity in the forms should go through your change management process
- 🐘 All code going through the forms should be subject to a peer review before it is entered
- 🐘 All activity within the forms should be audited using a trigger or log-based solution
- 🐘 All activity should be reconciled back to approved activity
- 🐘 For unauthorized changes, appropriate actions must be taken to plug the holes

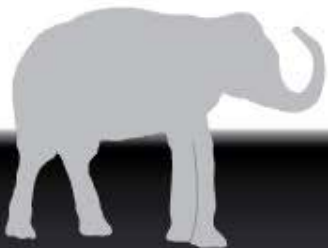


Accelerating the time for change in Oracle E-Business Suite



Configuration Change Management





- 🐘 ERP Systems – dormant code that is enabled through configurations
- 🐘 Impact of enabling functionality is same as 'development' activity
- 🐘 Do your policies and procedures acknowledge risks of changes to configurations having the impact of code change?
- 🐘 Have you performed a risk assessment to identify which configurations have the impact of code change?
- 🐘 Has your security been designed taking into account
- 🐘 Are you monitoring changes to configurations similar to ways you are/should be monitoring changes made through SDLC/object oriented development

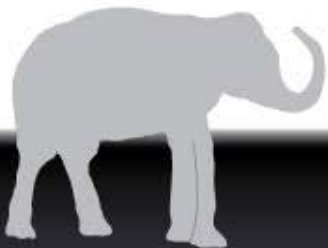


Accelerating the time for change in Oracle E-Business Suite



Types of Changes Subject to Change Management

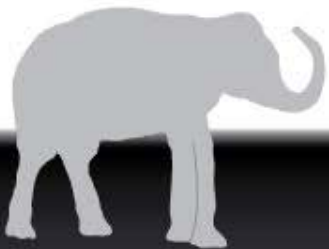
-  Development / SDLC
-  Patching
-  Security
-  Configurations



Accelerating the time for change in Oracle E-Business Suite



Questions?



Accelerating the time for change in Oracle E-Business Suite



Thank You!

Jeffrey T. Hare, CPA CISA CIA

ERP Risk Advisors | www.erpra.net

jhare@erpra.net | 970.324.1450

Answers from this session will be posted within two weeks on the LinkedIn Group,
EBS Answers: <http://www.linkedin.com/groups/EBS-Answers-4683349/about>



- One World, One System, A Single Source of Truth -



Accelerating the time for change in Oracle E-Business Suite

