
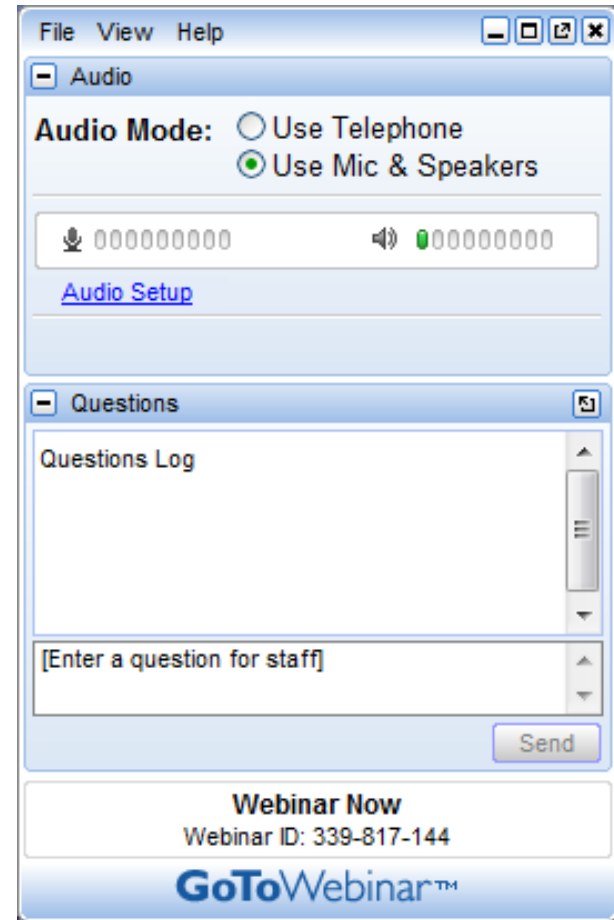

Auditing Oracle E-Business Suite Primer for Internal Auditors

Presented by:

Jeffrey T. Hare, CPA CISA CIA

Webinar Logistics

- Hide and unhide the Webinar control panel by clicking on the arrow icon on the top right of your screen
- The small window icon toggles between a windowed and full screen mode 
- Ask questions throughout the presentation using the chat dialog
- Questions will be reviewed and answered at the end of the presentation; I'll open the lines for interactive Q&A
- During the presentation, we will be conducting a number of polls, please take the time to respond to all those that are applicable
- CPE will only be give to those that answer at least 3 of the 4 polls



Presentation Agenda

Overview:

- Introduction
- Application Security Design
- IT Security
- SQL Forms and Utilities: Diagnostics
- Internal Controls and Security Deficiencies
- Sensitive Data in Non-Production Environments
- Application Controls
- Change Management
- Wrap Up
- Q&A

Introduction

Jeffrey T. Hare, CPA CISA CIA

- Founder of ERP Risk Advisors / ERP Seminars and Oracle User Best Practices Board
- Written various white papers on Internal Controls and Security Best Practices in an Oracle Applications environment
- Frequent contributor to OAUG's Insight magazine
- Experience includes Big 4 audit, 6 years in CFO/Controller roles – both as auditor and auditee
- In Oracle applications space since 1998– both as client and consultant
- Founder of Internal Controls Repository – public domain repository
- Author Oracle E-Business Suite Controls: Application Security Best Practices
- Contributing author Best Practices in Financial Risk Management
- Published in ISACA's Control Journal (twice) and ACFE's Fraud Magazine



Application Security Design

Application Security Design

Application Security Design:

- Risk-based approach
- Use principle of least privilege – was that how security was designed
- Use of standard menus and responsibilities
 - Upgrade risk
 - Excess access – value set maintenance, user profile values
- Use of standard request groups
- Review and understand security design process – are roles well understood by approvers, is single function risk as important of a concept at SOD risk?
- User provisioning process – do those that approve access understand details of roles and risks related to the access?

Application Security Design

Next Steps:

- View full webinar “Risk-Based Assessment of User Access Controls and Segregation of Duties for Oracle EBS” at <http://www.erpseminars.com/WebinarAccessForm.html>
- Level II Assessment: Software as a Service - Oracle E- Business Suite Segregation of Duties, Sensitive Function, and Sensitive Data Analysis
- Level II Assessment: Oracle E-Business Suite Privileged User Review
- Level II Assessment: Oracle E-Business Suite User Provisioning Process Review

Poll 1: How confident are you that your organization has fully addressed the risks related to application security?

IT Security

IT Security

IT Security:

- Following guidelines in 189367.1 and 403537.1
- Download primers from Integrigy and Solution Beacon
- Harden and re-harden after patches
- If implementing, hire a reputable EBS-specialized firm prior to go live.

Poll 2: How confident are you that your organization has fully addressed the risks spelled out in Oracle's Best Practices documents?

SQL Forms and Utilities: Diagnostics

Risks Related to SQL Forms

Risks related to SQL Forms

- Execution of any SQL Statements – insert, update, delete, select (DML) as well as database structure commands (DDL) – drop, truncate, alter, create, etc.; OS scripts
- Leading to fraud, data theft, taking over powerful accounts such as SYSADMIN, circumvention of policy such as change management, internal control deficiencies, additional audit fees, instability of application, etc.

Risk Related to SQL forms

Forms that accept SQL statements

- 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

Best Practices for monitoring activity in SQL forms

Forms that accept SQL statements

- See full webinar on SQL forms access at:
- <http://www.erpseminars.com/WebinarAccessForm.html>

Poll 3: Represents my organization's maturity related to SQL forms

Internal Controls and Security Deficiencies

Internal Controls and Security Deficiencies

Examples and Recommendations:

- Customers form, suppliers form, workflow history retention, lack of audit trail (before/after value) throughout the application, function deficiencies, lack of inquiry-only forms, global shared settings such as value sets, line types, profile classes, profile options, locations, customer header, supplier header
- May require forms to be personalized, trigger or log-based monitoring tool
- Sign up for the Internal Controls Repository at:
<http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/>

Sensitive Data in Non-Production Environments

Sensitive Data in Non-Production Environments

Sensitive data in non-production environments:

- Security is typically more loose in non-production environments
- May want to use post-clone steps to manipulate the data or secure the data
- Upcoming webinar on data security: Best Practices for Protecting Sensitive Data in an Oracle E-Business Suite Environment – Mar 18 11 a.m. EDT. Register: <https://www1.gotomeeting.com/register/321209880>

Application Controls

Application Controls Recommendations

For your application controls to be effective:

- Know your policies and procedures
- Know your process
- Make sure all system-related setups are documented and baselined
- Require changes to go through change management process – be documented and approved
- Ability to change setups and objects should be tightly controlled just as you control object changes
- Changes to setups and objects related to application controls should be audited
- Which... would require a detailed (log or trigger-based) audit trail to be built

Application Controls

Next Steps:

- See Auditing Application Controls webinar at:
<http://www.erpseminars.com/WebinarAccessForm.html>
- Level II Assessment: Oracle E-Business Suite SOX
Key Controls Best Practices Assessment.

Change Management

Change Management

Failure to take into account request groups access in design of security – request groups should be defined from the ground up for each responsibility as they allow for concurrent program access and access to sensitive data, some in standard request groups

Forms-based setups not being considered – some forms based setup changes have the impact of code change; change management is done to protect the integrity of the process

Change made in various forms that allow SQL statements embedded in them are not required to go through change management process – all activity in SQL forms should go through CM process, be audited and compared to SQL that has been peer-reviewed and was approved in the Change Management ticket (see list of forms in Internal Controls Repository and keep current with recommendations in Metalink Note 189367.1)

Change Management

Excessive access to forms requiring change management –

Example - Financials submenu in various menus and contains DFFs, KFFs, Value Set, Value Set Maint, Cross Validation Rules, Security Rules...

Failure to clearly document who is responsible for implementing change – Management should determine and document who are the appropriate Change Implementers

Failure to test for unauthorized changes – Anything that should go through CM process should be subject to audit. Need to develop a log or trigger based audit trail and compare to approved changes

Change Management

Failure to remediate issues that cause for unauthorized changes – need to do root cause analysis of unauthorized changes and remediate issues

Failure to maintain documentation – BR100s and BR110s should be kept current; user documentation; IT documentation; process documentation; internal controls testing; test scripts.

Poor impact analysis leading to a poor testing process – usually too much turf wars and not enough cooperation; requires tight cooperation between IT and functional users

Change Management

Next Steps:

- Level II Assessment: Oracle E-Business Suite Change Management Process Review

Wrap Up

Wrap Up

Recap

- Recorded webinars:

<http://www.erpseminars.com/WebinarAccessForm.html>

- Upcoming webinars / seminars:

<http://www.erpseminars.com/seminars.html>

- Intro Assessment: Level I Assessment: Assess Compliance with Provisions in the Oracle E-Business Suite
Controls: Application Security Best Practices book written by Jeffrey T. Hare, CPA CISA CIA

ERP Risk Advisory Services

- Free one-hour consultation
- On-site seminars (1 - 2 days) – custom tailored to your company's needs as well as various web-based seminars
- RFP / RFI management for Oracle-related GRC software
- SOD / UAC Third Party software projects / remediation
- GRC Software implementation
- Security and internal controls design and implementation for pre- and post-implementation
- Pre-defined level I and level II assessment services – see: <http://www.erpseminars.com/Services.html>

Q & A

Poll 4: I'd like the following follow up from this webinar:

Contact Information

Jeffrey T. Hare, CPA CISA CIA

- Cell: 970-324-1450
- Office: 970-785-6455
- E-mail: jhare@erpseminars.com
- Websites: www.erpseminars.com, www.oubpb.com
- Oracle Internal Controls and Security listserver (public domain listserver) at <http://groups.yahoo.com/group/OracleSox>
- Internal Controls Repository (end users only)
<http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/>
- Oracle GRC LinkedIn Group: www.linkedin.com/groups?gid=2017790
- Oracle ERP Auditors LinkedIn Group:
www.linkedin.com/groups?gid=2354934



Best Practices Caveat

Best Practices Caveat

The Best Practices cited in this presentation have not been validated with your external auditors nor has there been any systematic study of industry practices to determine they are ‘in fact’ Best Practices for a representative sample of companies attempting to comply with the Sarbanes-Oxley Act of 2002 or other corporate governance initiatives mentioned. The Best Practice examples given here should not substitute for accounting or legal advice for your organization and provide no indemnification from fraud, material misstatements in your financial statements, or control deficiencies.