Risk-Based Assessment of User Access Controls and Segregation of Duties for Companies Running Oracle Applications

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 questions window
- 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 given to those that answer at least 3 of the 4 polls
Presentation Agenda

Overview:
- Introductions
- Deficiencies in Current Approaches to SOD
- Taking a Risk-Based Approach to User Access Controls
- Examples
- Outcome of Typical Risk Assessment Projects
- Release 12 impact on SOD / UAC
- ERP Seminars SaaS SOD Offering
- Q&A
- Wrap Up
Introductions

Jeffrey T. Hare, CPA CISA CIA

• Founder of ERP Seminars and Oracle User Best Practices Board
• 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; 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
• Written various white papers on Internal Controls and Security Best Practices in an Oracle Applications environment
Deficiencies in Current Approaches to SOD Projects

Here are some common deficiencies in how companies are approaching SOD projects:

• Relying on seeded content of software providers

• Not taking a risk-based approach, considering current controls, in defining what risks are for their company

• Not considering all user access control risks – access to sensitive functions and access to sensitive data

• Always looking at risks as one function in conflict with another, rather than looking at real risks – single function and two functions

• Looking at SOX risks and ignoring some fraud risks below the materiality level
Poll 1

Represents my organization’s maturity related to SOD:
- We rely on seeded content from software provider
- We rely on risk advisor firm for our content
- We’ve done a thorough risk assessment internally
- We’ve done a thorough assessment including sub-material fraud risks
- None of these apply

- Check all that apply
Taking a Risk-Based Approach to User Access Controls

The *Original* Integrated Audit

- The original integrated audit – not the SOX type…
- Not looking at business process risk holistically – from outside the system through access and processes inside the system. Examples: suppliers, AR write offs, access to cash, access to check stock, account reconciliations
Taking a Risk-Based Approach to User Access Controls

Types of Risks:
Segregation of duties - a user having two or more business processes that could result in compromise of the integrity of the process or allow that person to commit fraud

Access to sensitive functions – a user having access to a function that, in and of itself, has risk

Access to sensitive data – a user having access to sensitive data such as employee identification number (US= SSN), home addresses, credit card, bank account information, plus data unique to your company – customers, BOMs, routings… ???
Poll 2

My organization has taken into account single function risks and risks related to access to sensitive data:

- Yes
- No
Taking a Risk-Based Approach to User Access Controls

Approach to Risk Assessment Project:
1. Identify access control conflicts
2. Identify risks associated with each conflict
3. Identify, analyze, and document mitigating controls related to each risk
4. Assess what is the residual risk after taking into account the mitigating controls
5. Discuss residual risks with management and assess their willingness to assume the risk
6. Document remediation steps for unmitigated risks
7. Document whether the conflict (single or combination of two) should be monitored in third party software
8. Document requirements for auditing software
Examples

• Spreadsheet – others’ approaches vs our approach
• Spreadsheet – other conflicts evaluated (OCE)
• Spreadsheet - assessment process examples
Current ERP Seminars Conflicts

• Conflicts across the following processes – Financial Close, Procure to Pay, Order to Cash, Hire to Pay, System Administration, Inventory Management

• Over 600 conflicts based on over 300 unique business processes (1000s of functions), including various critical manual processes such as Access to Cash, Access to Check Stock, Account Reconciliations, and Supplier Approval/Validation

• Evaluated over 1300 other conflicts from various audit firms

• Takes into account traditional SOD (user having two functions), single function risks, and access to sensitive data

• Significant portion of the risks can and should be applied to any ERP or legacy system
Taking a Risk-Based Approach to User Access Controls

In our experience, a completed risk assessment process exposes the following needs:

• An SOD monitoring tool (or one with a preventive workflow)
• Requirements for a trigger-based detailed audit trail
• Various monitoring reports or processes not provided by Oracle
• The need to personalize forms to support defined controls.
• Custom workflows to automate controls where Oracle’s functionality is deficient
• Process and/or controls changes
• Documentation and testing of non-key controls
• Access control / security changes
• Additional projects and research that need to be done (customizations, profile options, updating BR100s, BR110s, etc.)
Based on control requirements, we’ve done the following development

• Forms Personalization(s)
• Custom report(s) to supplement Oracle reporting
• Custom workflow(s)
• Implemented trigger-based auditing tool
• Other
Taking a Risk-Based Approach to User Access Controls

Typical high risk single functions:
• Foundation / Security / Development
  • Security Profiles, Roles, Responsibilities, Menus, Request Groups, Approvals Management, Functions, Executables, Concurrent Programs, Profile Option Values, Locations
• SQL Forms
  • Dynamic Trigger Maintenance, Alerts, Create Profile Options, Collection Plans (Quality) – over 30 forms
Taking a Risk-Based Approach to User Access Controls

Typical high risk single functions:

• Financial Close

• Hire to Pay
  • Elements, Security Profiles, Formulas, Approval Hierarchies, Enter Employees, Direct Deposit, Employee Addresses
Taking a Risk-Based Approach to User Access Controls

Typical high risk single functions:

• Order to Cash
  • Customers, Price Lists, Order Types, AR Transaction Types, System Options, Remit-To Addresses, Item Master, Receivables Activities, Adjustment Approval Limits, Access to Incoming Cash, Bank Reconciliation, Price List Security, Prepare Deposit, AR Adjustments, Adjustment Approval Limits, Credit Hold Release, Pricing Agreements, Pricing Formulas, Collection Activities, Enter Credit Memos, Claims Approval Limits
Taking a Risk-Based Approach to User Access Controls

Typical high risk single functions:

• Procure to Pay
  • Enter Suppliers, Approve Suppliers, Bank Accounts, AutoCreate Documents, Document Types, Line Types, Financial Options, Payables Options, Receiving Options, Purchasing Options, Qualifier Groups, Sourcing Rules, Buyers, Price Tolerances, Approval Groups, Item Master, Access to check stock, Initiate / Approve Wires

• Inventory Management
  • Item Master Maintenance, Item Cost Maintenance, Define Cycle Counts, Mass Edit Costs, Misc Inv Transactions, Define Phys Inventories
Taking a Risk-Based Approach to User Access Controls

However… Some functions do not exist:
• Procure to Pay
  • Blanket PO’s, Contract PO’s, Approve PO’s, Approve Req’s,
• Order to Cash
  • Credit limit maintenance, Order – price maintenance, Enter Credit Memo or RMA order, enter AR adjustments, Approve AR adjustments
• Hire to Pay
  • Maintain direct deposit, maintain employee address, enter salary, approve salary

And some functions do not tell the whole picture:
• Cash Management - Bank reconciliation versus manual process o/s system
• Procure to Pay - Enter Suppliers versus approval o/s system
• Order to Cash – Enter AR adjustments versus approval o/s system
Taking a Risk-Based Approach to User Access Controls

Typical high risk SOD conflicts:

• Overall – setups such as approval limits and hierarchies in conflict with the transactions they support

• Financial Close
  • Enter journals vs. post journals, journal sources, and authorization limits

• Procure to Pay
  • Enter suppliers vs. enter invoices
  • Enter payments vs. Payables options, bank accounts, bank reconciliation

• Hire to Pay
  • Run payroll vs. enter employee/convert applicant, maintain salaries
  • Enter employee/convert applicant vs. element entry
Taking a Risk-Based Approach to User Access Controls

Typical high risk sensitive data:
- Employee information such as SSN/National ID, bank account, addresses, garnishment information
- Customer information such as address, credit card, bank account
- Supplier information such as address, credit card, bank account
- Bill of Materials, Routing
- Some of this data can be accessed in inquiry only forms and some can be accessed by drilling into AP from various systems
Release 12 Impact on SOD and User Access Controls
Release 12 Impact on SOD/UAC

• Multi-org Access Control (MOAC) – broadens a user’s ability to update and inquire data across multiple OU’s and increases sensitivity of Security Profile changes (MO: Security Profile) – enables shared services
• Oracle Payments moving to TCA
• Suppliers and Banks move to TCA
• Reporting across OUs – sensitive information more easily obtained across all OUs
• Access to Supplier Maintenance from Buyer’s Workbench (upgrade risk!)
• Access to Enter Journals from various subledger setup menus (upgrade risk!)
ERP Seminars SaaS Offering
ERP Seminars SaaS Offering

SOD Scan Overview
Top 10 Analysis
Conflicts by User
Conflicts by Responsibility
Conflicts by Function
Conflicts by Rule
Conflicts by Menu
Conflicts
Intra-Responsibility Conflicts
Intra-Menu Conflicts
User Usage
Upload Your Data
Upload History
Links
Contact Caosys
Logout

CS*Proviso SaaS Portal: Caosys Limited - Test Account (CAOSYS)
SOD Scan Overview

<table>
<thead>
<tr>
<th>Scan Date</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Total Conflicts</th>
<th>Users</th>
<th>% Conflicts</th>
<th>Responsibilities</th>
<th>% Conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/08/2009</td>
<td>546</td>
<td>1.018</td>
<td>300</td>
<td>178</td>
<td>2.142</td>
<td>118</td>
<td>13</td>
<td>11.01</td>
<td>825</td>
</tr>
<tr>
<td>16/08/2009</td>
<td>2,199</td>
<td>2,948</td>
<td>3,472</td>
<td>1,082</td>
<td>5,701</td>
<td>118</td>
<td>14</td>
<td>11.86</td>
<td>825</td>
</tr>
<tr>
<td>01/08/2009</td>
<td>4,199</td>
<td>2,948</td>
<td>3,472</td>
<td>1,082</td>
<td>11.701</td>
<td>118</td>
<td>59</td>
<td>50.00</td>
<td>825</td>
</tr>
<tr>
<td>21/07/2009</td>
<td>5,199</td>
<td>3,948</td>
<td>3,472</td>
<td>1,082</td>
<td>13.701</td>
<td>118</td>
<td>59</td>
<td>50.00</td>
<td>825</td>
</tr>
</tbody>
</table>

Records 1 to 4 of 4

Critical Rank Conflicts

High Rank Conflicts

© 2007-2009 ERPS
ERP Seminars SaaS Offering

CS*Proviso SaaS Portal: CaoSys Limited - Test Account (CAOSYS)

Top 10 Analysis

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Conflicts</th>
<th>User</th>
<th>Conflicts</th>
<th>Function</th>
<th>Conflicts</th>
<th>Rule</th>
<th>Conflicts</th>
<th>Menu</th>
<th>Conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payables, Vision Operations (USA)</td>
<td>753</td>
<td>SKATZBERG 1,072</td>
<td>Suppliers</td>
<td>332</td>
<td>P0033</td>
<td>348</td>
<td>AP_APXINWKB_MENU</td>
<td>297</td>
<td></td>
</tr>
<tr>
<td>Application Developer</td>
<td>591</td>
<td>SOD_TEST_03 281</td>
<td>Daily Rates</td>
<td>162</td>
<td>P0079</td>
<td>303</td>
<td>AIN_PR PROCUREMENT</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>Purchasing, Vision Operations (USA)</td>
<td>319</td>
<td>CAOSYS 197</td>
<td>AutoCreate Documents</td>
<td>146</td>
<td>P0036</td>
<td>150</td>
<td>AIN_PR_PAYABLES</td>
<td>192</td>
<td></td>
</tr>
<tr>
<td>Payables Manager</td>
<td>281</td>
<td>SYSAVAN 197</td>
<td>Purchase Orders</td>
<td>138</td>
<td>P0034</td>
<td>123</td>
<td>AP_SUPPLIERS_GUI</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>Purchasing Super User</td>
<td>183</td>
<td>POLAND 197</td>
<td>Narga Suppliers</td>
<td>130</td>
<td>P0065</td>
<td>199</td>
<td>AP_INVOICES_ENTRY_GUI</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Implementation Financials</td>
<td>116</td>
<td>BADAMS 183</td>
<td>Invoices</td>
<td>105</td>
<td>P0002</td>
<td>90</td>
<td>AP_APXINWKB_VIEW_MENU</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Collections Forms Administrator</td>
<td>12</td>
<td>WIZARD 116</td>
<td>Receipts</td>
<td>71</td>
<td>P0035</td>
<td>87</td>
<td>Supply Base Management</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>Supplier Portal Full Access</td>
<td>6</td>
<td>COLLUSER 12</td>
<td>Receiving Transactions</td>
<td>93</td>
<td>P0018</td>
<td>83</td>
<td>AP_APXIPAWK_BATCHE_MENU</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Training Administrator</td>
<td>6</td>
<td>LSJHANSON 9</td>
<td>Invoice Holds</td>
<td>91</td>
<td>P0022</td>
<td>80</td>
<td>Purchase Orders Summary: Subfunctions</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>UK OTA Manager</td>
<td>4</td>
<td>SPROUTY 6</td>
<td>Invoice Actions</td>
<td>51</td>
<td>P0080</td>
<td>80</td>
<td>Setup: Currencies</td>
<td>76</td>
<td></td>
</tr>
</tbody>
</table>

Records 1 to 10 of 10

Top 10 by Response

- Payables, Vision Operations (USA)
- Application Developer
- Purchasing, Vision Operations (USA)
- Payables Manager
- Purchasing Super User
- Implementation Financials
- Collections Forms Administrator

© 2007-2009 ERPS
ERP Seminars SaaS Offering
ERP Seminars SaaS Offering

![SaaS Portal Image]

### Intra-Menu Conflict Pairs

<table>
<thead>
<tr>
<th>Menu</th>
<th>Rank</th>
<th>Conflicts (*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP_SUPPLIERS_GU12</td>
<td>Critical</td>
<td>6</td>
</tr>
<tr>
<td>AZN_PR_PAYABLES</td>
<td>Critical</td>
<td>5</td>
</tr>
<tr>
<td>Supply Base: Management</td>
<td>Critical</td>
<td>4</td>
</tr>
<tr>
<td>AZN_PR PROCUREMENT</td>
<td>High</td>
<td>50</td>
</tr>
<tr>
<td>AZN_EXPENSE_CYCLE</td>
<td>High</td>
<td>9</td>
</tr>
<tr>
<td>AZN_PR_ORDER_FULFILLMENT</td>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>AZN_PR_OE</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>AZN_PR_PAYABLES</td>
<td>Medium</td>
<td>5</td>
</tr>
<tr>
<td>AZN_PR_PAYABLES</td>
<td>Medium</td>
<td>2</td>
</tr>
</tbody>
</table>

Record 1 to 9 of 9 Page Size 20
Q & A
Poll 4

Question: Require any follow up from today's webinar

• I need a CPE certificate
• I'd like to set up a follow up call with Jeffrey
• I'd like to understand available SOD monitoring tools and/or trigger-based auditing solutions
• I'd like copies of the slides
• None necessary
Oracle Apps Internal Controls Repository

Internal Controls Repository Content:
• White Papers such as Accessing the Database without having a Database Login, Best Practices for Bank Account Entry and Assignment, Using a Risk Based Assessment for User Access Controls, Internal Controls Best Practices for Oracle’s Journal Approval Process
• Oracle apps internal controls deficiencies and common solutions
• Mapping of sensitive data to the tables and columns
• Identification of reports with access to sensitive data
• Recommended minimum tables to audit
• http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/
• Not affiliated with Oracle Corporation
ERP Seminars Services

• Free one-hour consultation
• On-site seminars (1 - 2 days) – custom tailored to your company’s needs
• Various web-based seminars
• RFP / RFI management for Oracle-related third party software
• SOD / UAC Third Party software project management
• SOD / UAC remediation prioritization
• Controls review related to Oracle-related controls – implementations and post-implementation
Seminars Offered and Planned

Seminars offered:

- Internal Controls and Application Security Best Practices in an Oracle e-Business Suite Environment
- Application Security Design: Fundamentals
- Application Security Design: Advanced Concepts
- Implementing Oracle e-Business Suite: Internal Controls Challenges
- Introduction to Oracle’s User Management Module and Related Risks
- Auditing Oracle E-Business Suite: Application Security
- Monitoring Privileged Users in an Oracle E-Business Suite Environment
- Risk-Based Assessment of User Access Controls and Segregation of Duties for Companies Running Oracle E-Business Suite

Seminars planned:

- User Management: How To
- Auditing Oracle E-Business Suite: Top Internal Controls and Security Risks
- Auditing Oracle E-Business Suite: Internal Controls Deficiencies
- Upgrading to Release 12: Internal Controls and Security Issues
About ERP Seminars

• Thought Leadership, Best Practices

• Aggregator of public domain content and best practices

• A hands-on, Oracle Applications focused analyst firm - but not an analyst firm that only covers those pay for coverage

• NOT a consulting firm, although I do some limited consulting

• Independent of any 3rd party software – attempt to cover all relevant solutions in the Oracle Apps ‘Controls Automation’ space
Contact Information

Jeffrey T. Hare, CPA CISA CIA

- Cell: 970-324-1450
- Office: 970-785-6455
- E-mail: jhare@erpseminars.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/
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.