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

Presented by:

Jeffrey T. Hare, CPA CISA CIA

ERP Seminars

Presentation Agenda

Overview:

- Introductions
- Deficiencies in Current Approaches to SOD
- Taking a Risk-Based Approach to User Access Controls
- Q&A
- Public Domain Collaboration
- Oracle Apps Internal Controls Repository
- OUBPB / ERP Seminars Initiatives
- Other Resources
- Contact Information

Introductions

Jeffrey T. Hare, CPA CISA CIA

- Founder of ERP Seminars and Oracle User Best Practices Board
- Written various white papers on SOX 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 auditor and audited perspectives
- In Oracle applications space since 1998– both client and consultant perspectives
- Founder of Internal Controls Repository - public domain internal controls repository for end users

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 there are for their company
- Not considering all user access control risks – access to sensitive functions and access to sensitive data
- 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
- Not having a good grasp on requirements for the RFP

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 high risk 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, and/or bank account information.

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 of combination of access) should be monitored in third party software and use as basis for RFP

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)
- A tool to develop a 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 changes
- Additional projects and research that need to be done

Q & A

ERP SEMINARS

Public Domain Collaboration

What is needed are standards for collection of:

•Tables to audit as data is migrated (for example banks)

•Additional functions and functionality is added

Internal Controls Repository:
http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/

•Publishing list of critical forms, tables, columns to audit prioritized by risk

•Promoting use of our risk assessment process as the standard in the industry with agreement on language and mapped to the function level

Public domain collaboration will insure consistency and quality

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 table and columns
- Identification of reports with access to sensitive data
- http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/

Other Resources

- Oracle Users Best Practices Board: www.oubpb.com
- Cam's white paper on Auditing the DBA at: http://www.absolute-tech.com/products/whitepapers.htm
- Integrigy white papers at: http://www.integrigy.com/security-resources
- Solution Beacon: http://www.solutionbeacon.com/security.htm
- Oracle internal controls and security public listserver: http://tech.groups.yahoo.com/group/OracleSox/

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 or material misstatements in your financial statements or control deficiencies.

Contact Information

Jeffrey T. Hare, CPA CISA CIA

- Phone: 602-769-9049
- E-mail: jhare@erpseminars.com
- Websites: **www.erpseminars.com**, **www.oubpb.com**
- Oracle SOX eGroup at **http://groups.yahoo.com/group/OracleSox**
- Internal Controls Repository **http://tech.groups.yahoo.com/group/oracleappsinternalcontrols/**