Application Security Best Practices in an Oracle E-Business Suite Environment

Application Security best practices

Introduction - Jeffrey T. Hare, CPA CISA CIA

- Founder of ERP Risk Advisors
- Written various white papers on Internal Controls and Security Best Practices
- 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 1997– both client and consultant perspectives
- Founder of Internal Controls Repository – public domain repository
- Author:
  - Book Oracle E-Business Suite Controls: Application Security Fundamentals
  - Book: Auditing Oracle E-Business Suite: Common Issues

Why Good Role Design?

Proper application security and role design forms the foundation of your internal controls environment.

Poor role design during the implementation of ERP applications leads to excessive risk, Segregation of Duties issues, and audit findings.

Integrity of control design - those performing controls do not have access to transactions – basic Segregation of Duties

RESPONSIBILITIES / ROLE / ROLE DESIGN

- Based on principle of least privilege – only what is necessary for the persons(s) to do their job tasks
- SOD conflict free
- Each role should only include the sensitive data needed to be viewed by those with the role
- Each role should only contain sensitive / high risk functions needed to be accessed (data entry, setups, SQL forms, etc.)

RESPONSIBILITIES / ROLE / ROLE DESIGN

- User Management shouldn't be used except in certain limited circumstances. Don't start with the assumption that UMX will be used.
- Design one core Responsibility per job role – this would be a custom menu and custom request group that would be replicated across OUs
- You should not use standard menus in the development of custom menus for end users because of impact of Oracle patches on standard menus. AZN menus example.
- Use submenus in limited instances
- Don't use the big six IT responsibilities – App Dev, Sys Admin, Sys Administration, Alert Manager, Functional Developer, Functional Administrator

RESPONSIBILITIES / ROLE / ROLE DESIGN

- Perform risk assessment to identify which setups should be subject to the change management process and which should be managed by end users.
- Access to setups for end users (transactional) and IT (foundational) should only be provided in a custom submenu, never use the standard setup submenus
- Limit access to setup menus in UAT environment to keep it ‘clean’.
- Proper risk analysis between old and new security when patching and ESPECIALLY during major upgrades.

RESPONSIBILITIES / ROLE / ROLE DESIGN

- Quality assurance process - Implementation of a trigger or log-based solution to develop audit history to provide complete system based audit trail, notifications for high risk areas, documentation of actual changes back to change management tickets
- Over elements that are subject to change control – Users, Resps, Menus, Request Groups, Functions, Forms, Concurrent Programs, Executables, Objects, AME, Functional Configuration Changes, Forms / pages that allow SQL injection, Profile Options, Profile Option Values.

RESPONSIBILITIES / ROLE / ROLE DESIGN

- User provisioning request form detail functionality within each role / responsibility and be a part of security Change Management process.
- Implement SoD tool like CaoSys' CS*Comply
- Perform Lookback Analysis where you have identified unauthorized access

RESPONSIBILITIES / ROLE / ROLE DESIGN

- Use a tool like CaoSys' CS*Provisum to fully automate the provisioning process and provide access to Segregation of Duties conflicts and Sensitive Access risks as part of the provisioning process.
- Use prevent-mode and approval rules during the provisioning process to reduce introducing SoD conflicts and Sensitive Access risks
- Re-validate security on a quarterly basis (CaoSys' CS*Provisum) – Supervisor, Process Owner, Rules in-scope for SOX.

Wrap Up, Q&A, Contact Information

Services and offerings

- VAR, Implementation Partner of CaoSys GRC software that competes with Oracle's GRC suite
- Covering over 1,000 SoD and Sensitive Access rules, nearly 3,000 functions, and nearly 1,500 high risk concurrent programs
- Application security design / redesign
- Audit support – particularly for application security and application controls

Services and offerings

- Health check / assessments – for IT or internal audit
- Pre-conference workshop at Collaborate 17
- Internal controls and security training through MISTI
  - 24-Apr-2017: New York
  - 21-Aug-2017: Anaheim
  - 09-Oct-2017: San Francisco

Jeffrey T. Hare, CPA CISA CIA

- Cell: 970-324-1450
- E-mail: jhare@erpra.net
- Website: www.erpra.net
- LinkedIn: www.linkedin.com/in/jeffreythare
- Twitter: @jeffreythare