

Change Management Best Practices in an Oracle E-Business Suite Environment

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

Agenda

Change management is a multi-faceted topic. Like the various sides of a gem, doing change management well requires various approaches. One can think of change management in four different buckets — object oriented changes, security, patching, and configurations.

What it takes to build and implement a first class change management process for organizations running Oracle E-Business Suite.

Types of Changes:

These are four unique types of changes all with different risks and processes:

- Object-oriented / development (at all levels)
- Security (at all levels)
- Patches (at all levels)
- Configuration (at all levels)

GTAG 2 – What Is It?

- Produced by the Institute of Internal Auditors
- Global Technology Audit Guide: Change and Patch Management Controls: Critical for Organizational Success
- Originally published in 2005 and updated in 2012

- Role Design – Are your roles designed with this in mind?
 - Only those employees that are authorized to make changes have access to make changes – DBAs, developers, Business Analysts, End Users
- Segregation of Duties between developed and migration to UAT and Prod

Change Management Roles

Table 4: Typical Roles

Roles in the Change Lifecycle	Typical Titles and Roles
Change requester	Business unit, IT operations, security, service manager.
Change preparer	R&D, database administrator, application development team, application programmer. Quality assurance, build and staging team, pre-production team, platform team.
Change approver	Change manager, change advisory board, change control committee, change management board.
Change implementer	IT operations, network operations, network engineering, systems administrators, security.
Change reviewer	IT operations management, change advisory board, security, auditing.
Change audit	IT operations management, change advisory board, security, auditing.

Change Management Segregation of Duties

Table 5: Segregation of Duties

For each change...	Should be independent of...
Implementers	Requesters
Operators of the production environment	Preparers
Tester	Preparers
Implementers	Preparers
At least one approver	Preparers
At least one approver	Requesters
At least one approver	Implementers
Reviewers	Implementers
Audit	All of the above

Segregation of Duties – Do your policies and procedures clearly spell these out?

- Requestor shall be independent of Implementer
- Preparer shall be independent of Requestor, Tester, Implementer, and Verifier
- Peer Reviewer shall be independent of Preparer and Implementer
- Implementer shall be independent of Requestor, Tester and Verifier

Common Change Management Challenges

- Lack of technology to build before / after value changes so Change Management audits have a population of changes from which to pull – Consider CaoSys CS*Audit in lieu of Oracle's CCG solution
- Excessive access to forms requiring change management / Failure to clearly document who is responsible for implementing change
- Lack of Segregation of Duties between development and migration to UAT and PROD – Alerts, Configurations

Common Change Management Challenges

- Change made in various forms that allow SQL statements embedded in them are not required to go through change management process – end user forms,
- Failure to remediate issues that cause for unauthorized changes
- Poor impact analysis leading to a poor testing process / software to identify changes to configurations
- Failure to re-harden the application after patches are applied / upgrades

Common Change Management Challenges

- Lack of Profile Options Risk Assessment – whether they are set, at what level they are set, who should approve
- Changes to security not being properly tested for SoD conflicts and Sensitive Access risks
- Lack of approach for high risk Concurrent Programs / Failure to take into account request groups access in design of security
- Lack of clear definition of what is considered sensitive data, where it is stored, and what objects can access it

Software you may be missing

- Trigger-based auditing solution like CaoSys' CS*Audit to build audit history for changes so quality assurance process can be implemented
- Access controls solution like CaoSys' CS*Comply to test for access to functions that should subject to change management
- Lookback analysis solution like CaoSys' CS*Comply to perform lookback analysis procedures when inappropriate access is identified for configurations subjects to change control

Software you may be missing

- Periodic access review solution like CaoSys' CS*Provisum to re-validate those with access to change management functions
- Impact analysis solution like Ringmaster to identify changes for properly testing
- Code management / code migration solution like Dell's Stat for source code management and migration
- Database security solution like Integrigy's AppSentry to test for re-hardening requirements after patches and test configuration of servers that are internet facing

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
- Internal controls and security training through MISTI
 - Class in San Francisco – 12-Dec to 14-Dec
 - <http://misti.com/event-details?EVENTID=14209&ORGCODE=10>

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