Change Management Best Practices for ERP Applications, An Internal Auditor's Perspective

Jeffrey T. Hare, CPA CISA CIA
ERP Risk Advisors
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
Presentation Agenda

Overview:

• Introduction
• GTAG 2: What is it?
• Internal Auditor Expectations
• Common Change Management Challenges
• Wrap Up / Q&A

Note: CPE will be offered for those that answer at least 4 (of the 5) polls presented during the webinar.
Introductions

Jeffrey T. Hare, CPA CISA CIA:
• Founder of ERP Risk Advisors / 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 – as client and consultant
• Founder of Internal Controls 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 and ACFE’s Fraud Magazine
Poll 1: Will you be needing a CPE Certificate?

- Yes
- No
- Not Sure
GTAG 2 – What is it?

- Global Technology Audit Guide: Change and Patch Management Controls: Critical for Organizational Success
Poll 2: How would you rate your Change Management maturity on a scale of 1 to 5 with 1 being not mature and 5 being very mature?

• Answer 1 - 5
# Change Management Metrics

<table>
<thead>
<tr>
<th>Metric and Indicators</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of changes authorized per week, as measured by the change management log of</td>
<td>In general, more changes indicate more change productivity, as long as the change success rate remains high. The trend (up, down or steady) should make sense in the business context. High-performing organizations can sustain over 1,000 successful changes per week.</td>
</tr>
<tr>
<td>authorized changes.</td>
<td></td>
</tr>
<tr>
<td>Number of actual changes made per week, as measured by detective controls such as</td>
<td>The number of changes actually implemented for the week should not exceed the number of authorized changes.</td>
</tr>
<tr>
<td>monitoring software.</td>
<td></td>
</tr>
</tbody>
</table>
## Change Management Metrics

<table>
<thead>
<tr>
<th>Metric and Indicators</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unauthorized changes. These are changes that circumvented the change process.</td>
<td>Lower is better, but typically the only acceptable number of unauthorized change is zero; one rogue change can kill an entire operation or create material risk.</td>
</tr>
<tr>
<td>This is measured by taking the number of actual changes made and subtracting the number of authorized changes.</td>
<td>Large numbers of unauthorized changes indicate that “the real way to make changes” is to circumvent the change management process.</td>
</tr>
<tr>
<td>Where detective controls are not present, no reliable measurement of actual changes can be made. In this case, the number of unplanned outages can be used as a substitute measure.</td>
<td>High-performing organizations have a culture of change management and consequently state that they do not tolerate any unauthorized changes.</td>
</tr>
</tbody>
</table>
## Change Management Metrics

<table>
<thead>
<tr>
<th>Metric and Indicators</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of emergency changes (including patches), determined by counting the number of changes that required an urgent approval during the week using the change review board or emergency change process.</td>
<td>Lower is typically better. Many emergency changes indicate that the “real way to make changes” is to use the emergency change process either for convenience or speed. Emergency changes typically have a higher failure rate and generate unplanned work or rework. An increase in emergency changes may indicate that there are other change management problems causing this increase. ITPI benchmarking found that when emergency changes comprise more than 10 percent of total changes, the organization is almost certainly a low performer. In particular, two organizations that had catastrophic “front page news” IT failures were typically expediting more than 25 percent of their change requests</td>
</tr>
</tbody>
</table>
## Change Management Metrics

<table>
<thead>
<tr>
<th>Metric and Indicators</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change success rate, defined as successfully implemented changes (those that did not cause an outage, service impairment, or an episode of unplanned work) as a percentage of actual changes made.</td>
<td>Higher is better. When changes are not managed and not adequately tested, change success rates typically are around 70 percent. High-performing organizations not only regularly achieve change success rates of 99 percent, but failed changes rarely cause service interruptions or unplanned work.</td>
</tr>
</tbody>
</table>
Segregation of Duties – do your policies and procedures clearly spell these out?

- Requestor shall be independent of Approver
- Preparer shall be independent of Requestor, Tester and Verifier
- Peer Reviewer shall be independent of Preparer and Implementer
- Implementer shall be independent of Requestor, Tester and Verifier
Internal Auditor Expectations

There is sufficient detail in the policies and procedures – are these types of changes delineated with enough detail. There are differences by the types of changes:

- Patching – at all levels
- Security – at all levels
- Configurations – at all levels, but particularly at the application level
- Objects / development

For each type of change, the roles are different.
# Change Management Role Examples

<table>
<thead>
<tr>
<th>Role</th>
<th>Configurations</th>
<th>Objects / SDLC</th>
<th>Security</th>
<th>Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester</td>
<td>Process owner</td>
<td>Process owner</td>
<td>Process owner</td>
<td>Applications owner</td>
</tr>
<tr>
<td>Preparer</td>
<td>Business Analyst</td>
<td>Development</td>
<td>Security Administrator</td>
<td>DBAs</td>
</tr>
<tr>
<td>Peer Reviewer</td>
<td>N/A</td>
<td>Development Peer</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Approver</td>
<td>Process owner</td>
<td>Process owner</td>
<td>Process owner</td>
<td>All Process Owners</td>
</tr>
<tr>
<td>Tester</td>
<td>Process owner</td>
<td>Process owner</td>
<td>Process owner</td>
<td>All Process Owners</td>
</tr>
<tr>
<td>Implementer</td>
<td>Business Analyst</td>
<td>DBAs</td>
<td>Security Administrator</td>
<td>DBAs</td>
</tr>
<tr>
<td>Verifier</td>
<td>Process owner</td>
<td>Process owner</td>
<td>Process owner</td>
<td>All Process Owners</td>
</tr>
</tbody>
</table>
Poll 3: We currently have these activities in place (multiple answers allowed)

- We have a system-based audit trail using logs or triggers.
- We have done a risk assessment re: configs going through CM.
- We have a QA process that looks for unapproved changes.
- We have separate procedures for all 4 types of changes.
- We have limited access to those authorized to make changes.
Exceptions to policies and procedures are approved by management and documented accordingly

- For example – when can generic accounts be used to apply patches or do other maintenance in the application.
- SYSADMIN should be called out as an exception if being used as is called for in some Oracle patches
Internal Auditor Expectations

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
Common Change Management Challenges

• Profile Options not being considered
• Changes to security not being considered
• Failure to take into account access to sensitive data in security process changes
• Failure to take into account request groups access in design of security
• Forms-based setups not being considered
Common Change Management Challenges

• Failure to identify and document which configuration are subject to the change management process, based on risk
  • Then, failure to restrict access only those that are authorized to make such changes
  • Security (Responsibilities, Menus, Functions)
  • Configurations related to key controls (Line Types, Document Types, AME)
  • Foundational configurations (DFF, KFF, Objects)
  • Configurations subject to fraud (Locations, Remit To Addresses)
## Common Change Management Challenges

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Generation Processes</td>
<td>Forms</td>
<td>Special Information Types</td>
</tr>
<tr>
<td>Accounting Setup Manager</td>
<td>Functions</td>
<td>Extra Information Types</td>
</tr>
<tr>
<td>Applications</td>
<td>Key Flexfield Setups</td>
<td>Fast Formulas</td>
</tr>
<tr>
<td>Approvals Management (AME)</td>
<td>Document Sequences</td>
<td>Data Access Sets</td>
</tr>
<tr>
<td>AutoAccounting Rules (PA)</td>
<td>Hold and Release Names</td>
<td>Definition Access Sets</td>
</tr>
<tr>
<td>Bank Statement Mapping</td>
<td>Tolerances</td>
<td>Journal Sources</td>
</tr>
<tr>
<td>Bank Statement Transaction Codes</td>
<td>Write Formula</td>
<td>System Parameters (CE)</td>
</tr>
<tr>
<td>All forms that accept SQL statements</td>
<td>Concurrent Programs (System Administrator Mode)</td>
<td>Maintain Security Profiles / Assign Security Profiles</td>
</tr>
<tr>
<td>Concurrent Program Executables</td>
<td>Subledger Accounting Setups</td>
<td>Fast Formulas</td>
</tr>
<tr>
<td>Book Controls (Assets)</td>
<td>Task Flow Nodes</td>
<td>Maintain Elements</td>
</tr>
<tr>
<td>Data Groups</td>
<td>Task Flow Definitions</td>
<td>Payables Options</td>
</tr>
<tr>
<td>Define Query Objects</td>
<td>Task Flow Units</td>
<td>Financials Options</td>
</tr>
<tr>
<td>Descriptive Flexfield Setups</td>
<td>Global Organization Hierarchy</td>
<td>Payables System Setup</td>
</tr>
<tr>
<td>Dynamic Trigger Maintenance</td>
<td>Security Profiles</td>
<td>Lookups</td>
</tr>
<tr>
<td>Forms Configurator</td>
<td>Global Security Profile</td>
<td>Alerts</td>
</tr>
<tr>
<td>Contexts</td>
<td>Information Types Security</td>
<td>Profile Option Values</td>
</tr>
<tr>
<td>Transaction Status</td>
<td>Form Customization</td>
<td>Menus</td>
</tr>
<tr>
<td>Request Groups</td>
<td>Value Sets</td>
<td>Organizations</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>Locations</td>
<td>User Management Roles</td>
</tr>
<tr>
<td>Profile Options</td>
<td>Accounting Setup Manager</td>
<td></td>
</tr>
</tbody>
</table>

© 2012 ERPRA
Common Change Management Challenges

• Changes made in various forms that allow SQL statements embedded in them are not required to go through change management process – Alerts, Collection Plans, Deletion Statements, etc
• Excessive access to forms requiring change management
• Failure to clearly document who is responsible for implementing change
• Failure to test for unauthorized changes
Common Change Management Challenges

- Failure to properly QA change management process
- Lack of technology to build before / after value changes so Change Management audits have a population of changes from which to pull
- Failure to remediate issues that cause for unauthorized changes – root cause analysis
- Failure to maintain documentation – SoD matrix, list of customization, changes to process documentation, training documentation
Common Change Management Challenges

• Poor impact analysis leading to a poor testing process because impact of changes not properly evaluated
  • Relying on Read Me file
• Failure to identify the impact of patches
  • Objects
  • Data
  • Security – Applications / Database
  • Configuration
• Failure to re-harden the application after patches are applied
Poll 4: These activities through the forms are subjects to Change Management (multiple answers allowed)

- All security changes (menus, resps, rqst groups, functions)
- All development changes (objects, workflow)
- Configurations related to key controls
- Foundational configurations
- Forms that allow SQL statements embedded in them
Questions and Answers
Poll 5: Will you be needing a CPE Certificate?

- Yes
- No
Resources

• Jeffrey Hare’s book “Oracle E-Business Suite Controls: Application Security Best Practices” – available at Collaborate bookstore; online

• www.erpra.net
Oracle Apps Internal Controls Repository

Internal Controls and Security Public Domain Repository

Sample of content:
  • White papers
  • Sample development specs
  • Sample forms personalizations
  • Sample policies and procedures
  • SQL Training Docs
  • Forms that Allow SQL Statements
  • List of Generic Application Users
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:
- Cell for Jeff: 970-324-1450
- E-mail: jhare@erpra.net
- Website: www.erpra.net
- Website: www.oubpb.com
- Skype: jhareaz
- LinkedIn: http://www.linkedin.com/in/jeffreythare
- Twitter: http://twitter.com/jeffreythare
- LI Groups: Oracle GRC, Oracle ERP Auditors