YEAR-END GAAP REPORTING TRAINING

IT AUDIT

Amy Vuong, Director, KPMG LLP

April 8, 2016
KPMG IT Audit FY 2014-15 Results

- In Scope Systems
  - Common Financial System (CFS) – Effective

- Findings
  - 5 total IT deficiencies
## Prior Year IT Findings (1 of 5)

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>Exists as of 6/30/15</th>
<th>Management Response</th>
<th>Root Cause for the Finding</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| **Password Policy & Configuration:**  
KPMG noted that the CSU Access Control Standard requires all campuses to identify and implement strong password criteria including criteria for minimum password length, complexity, failed attempts, and aging schedule. The Sacramento campus does not have any password policy or configuration requirements for complexity, maximum number of failed attempts, or remembered passwords. | Yes (Sacramento - Yes  
CO - Yes  
Northridge - No) | The Chancellors Office concurs. The CISO will send a memo to all campus CIO and ISO’s reiterating the password policy and requirements and to ensure configurations match stated campus policies. CSU Sacramento has submitted their changes and response. | Non-adherence to policies and procedures | The password configurations established at each campus should be reviewed/updated to reflect the requirements stated in the Access Control Standards document and the campus password policies. |
| **Password Configuration:**  
- The password configurations at the Chancellor’s Office did not adhere to the CO’s password policies. More specifically, we noted that the policy on failed password attempts denoted a maximum of 5 attempts, while the configuration was set at 6 attempts.  
- The password configurations at CSU Northridge did not adhere to their password policies. We noted that the policy on password history denoted 6 remembered passwords, while the configuration was set at 5 remembered passwords. | | | | |
## Prior Year IT Findings (2 of 5)

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>Exists as of 6/30/15</th>
<th>Management Response</th>
<th>Root Cause for the Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CFS Oracle Database Passwords:</strong></td>
<td></td>
<td>Yes</td>
<td>Non-adherence to policies and procedures</td>
<td>The password policies and configuration should be updated to reflect the</td>
</tr>
<tr>
<td>There are no password criteria being enforced for the</td>
<td></td>
<td>The Chancellors Office Conurs. CFS user account, service account and PeopleSoft</td>
<td></td>
<td>requirements stated in the system-wide policy.</td>
</tr>
<tr>
<td>CFS production database.</td>
<td></td>
<td>account password parameters have been determined and will be implemented by March</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2016. Additionally the CO password policy has been updated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


*Note: The details above are for a specific finding related to CFS Oracle Database Passwords. Further details and updates are provided in the management response section.*
## Prior Year IT Findings (3 of 5)

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>Exists as of 6/30/15</th>
<th>Management Response</th>
<th>Root Cause for the Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOD Review:</strong> KPMG noted that CSU Fullerton did not complete the monthly SOD review for December.</td>
<td>Yes</td>
<td>The Chancellors Office concurs. The CISO will send a memo to campus CIO and ISO’s reminding them of the SOD policy and timeliness in completing required reports.</td>
<td>Non-adherence to policies and procedures</td>
<td>Policies and procedures must be followed in order for processes to be deemed effective. Review the established process and ensure that campuses are following the procedures as documented.</td>
</tr>
</tbody>
</table>
**Prior Year IT Findings (4 of 5)**

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>Exists as of 6/30/15</th>
<th>Management Response</th>
<th>Root Cause for the Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminations:</strong>  KPMG noted that there were a number of terminated users whose access was not removed in a timely manner (10 days from their termination date) from CFS.  - Fullerton: 2 users (71 and 216 days)  - Sacramento: 5 users (12, 19, 24, 44, 309 days)  - San Jose: 4 users (18, 21, 26, 116 days)  - San Luis Obispo: 4 users (12, 13, 14, 25 days)</td>
<td>Yes</td>
<td>The Chancellors Office concurs. The CIO will send a memo to campus CIOs and ISO's stating the need for timely (within 10 business day) termination of access.</td>
<td>Non-adherence to policies and procedures</td>
<td>A general timeline should be implemented on how quickly a terminated user should be removed from the system. KPMG will be testing the removal/disabling of access for terminations within a one week timeframe after the termination date. The majority of campuses do not conduct a regular review over terminated users. Campuses should implement a regular review process to catch terminated users that were not disabled within one week.</td>
</tr>
</tbody>
</table>
# Prior Year IT Findings (5 of 5)

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>Exists as of 6/30/15</th>
<th>Management Response</th>
<th>Root Cause for the Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GAAP Override Access:</strong> KPMG noted one shared user account, Sacramento Production Process, with access to the GAAP override function that does not require this access and should be removed.</td>
<td>No</td>
<td>No action needed.</td>
<td>Lack of user access review</td>
<td>A periodic review of users with GAAP override access should be performed.</td>
</tr>
</tbody>
</table>
KPMG IT Audit – Approach

• Perform IT Audit for FY 2015 -16
  • IT General Controls
  • IT Application Controls

• Purpose
  • Gain assurance over internal controls in place over IT systems to limit the risk of material misstatement to the financial statements
  • Reliance on IT system controls over computerized output reduces substantive procedures required for financial statement audits
KPMG IT Audit – Scope of Work

- In Scope System
  - Common Financial System (CFS)
- Current year procedures are in the process of being conducted at the following locations:
  - Chancellor’s Office
  - Fullerton
  - Long Beach
  - Northridge
  - Pomona
  - San Francisco
  - San Jose
  - San Luis Obispo
KPMG IT Audit – Overview of IT General Controls

• IT General Controls
  • Controls that support the foundation of the system.
  • Includes 4 components:
    • Access to Programs and Data
    • Program Changes
    • Program Development
    • Computer Operations
KPMG IT Audit – IT General Controls Procedures

• Access to Programs and Data
  • IT Security Policies
  • Passwords
  • Security Access Rights / Privileged Access
  • DBA Access
  • Granting / Modifying Access
  • Terminating Access
  • Physical Access
  • Annual User Access and SOD Review
KPMG IT Audit – IT General Controls Procedures

• Program Changes
  • Change Management Policies and Procedures
  • Change Management Request and Approval
  • Change Management Testing
  • Change Management Security Access Rights
KPMG IT Audit – IT General Controls Procedures

• Computer Operations
  • Job Processing
  • Backup Procedures
  • Restoration Testing
  • Access to Backup Tapes
  • Incident Management
KPMG IT Audit – Overview of IT Application Controls

• Application Controls – are automated controls or manual controls with an automated component
  • Steps, **requirements**, that a computer system executes to achieve a specific **objective**—the objective of the automated control to prevent, detect and/or correct the risk of a financial misstatement

• Types of IT Application controls include:
  • system configuration/account mapping
  • exception/edit reports, including review of these reports
  • interface controls, and
  • system access, including enforcing segregation of duties.

• If the IT General Controls are operating effectively → KPMG IT will conduct testing over select IT Application Controls
KPMG IT Audit – IT Application Controls Procedures

• IT Application Controls
  • Current year procedures include:
    • Journal Entries Completeness testing
    • Access to enter/post Journal Entries
    • GAAP Derivation process
    • Access to the GAAP Override feature
KPMG IT Audit – Deficiency and Communication

• Control deficiencies
  • Confirm deficiencies with control owners before finalizing and reporting
  • Perform additional testwork/identify compensating controls to mitigate the risk
  •Perform remediation procedures
KPMG IT Audit – Deficiency and Communication

• Impact on Financial Audit Team
  • As the IT team leads in their testwork timing, KPMG IT will report all deficiencies to the financial audit team.
  • The financial audit team will analyze these deficiencies as they relate to the year-end financial statement audit and modify the audit approach as may be necessary. This may include performing additional substantive procedures, making additional sample selections, etc.
# KPMG IT Audit – Key Dates

<table>
<thead>
<tr>
<th>Task</th>
<th>Day</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPMG to provide PBC Request Lists to CSU</td>
<td>Friday</td>
<td>April 8, 2016</td>
</tr>
<tr>
<td>CMS and Campus to provide PBC items to KPMG</td>
<td>Monday</td>
<td>April 25, 2016</td>
</tr>
<tr>
<td>On-site fieldwork begins</td>
<td>Monday</td>
<td>April 25, 2016</td>
</tr>
<tr>
<td>KPMG will perform testwork over IT General Controls and IT Application Controls</td>
<td></td>
<td>April 25, 2016 – June 30, 2016</td>
</tr>
<tr>
<td>Rollforward Testing / Project Wrap up / Close out Meeting</td>
<td></td>
<td>July 2016</td>
</tr>
</tbody>
</table>