MAYOR JIM GRAY

LEXINGTON

BRUCE SAHLI
DIRECTOR
OFFICE OF INTERNAL AUDIT

MANAGEMENT ACTION PLAN PROGRESS REPORT

DATE: July 18, 2017

TO: Jim Gray, Mayor

CC: Sally Hamilton, Chief Administrative Office
Glenn Brown, Deputy Chief Administrative Officer
Aldona Valicenti, Chief Information Officer
William O'Mara, Commissioner of Finance & Administration
Phyllis Cooper, Director of Accounting
Phillip Stiefel, Director of Enterprise Solutions
Susan Straub, Communications Director
Urban County Council
Internal Audit Board

FROM: Bruce Sahli, CIA, CFE, Director of Internal Audit
Matthew Reid, CPA, Internal Auditor

RE: Journal Entry Controls Audit MAPPR

Background

On June 20 2016, the Office of Internal Audit issued the Journal Entry Controls Audit Report. The 2016 audit report contained findings related to the lack of a journal entry audit trail, the excessive number of employees with journal entry capabilities, the methodology of updating user roles in PeopleSoft as job duties change, and communicating changes in employment status to the Division of Enterprise Solutions (DES). The scope of the audit included activity for the period January 1, 2013 through December 31, 2015.

This review is provided for management information only. It is not an audit and no opinion is given regarding controls or procedures. We interviewed staff from the Division of Accounting and Division of Enterprise Solutions, and obtained other evidence as necessary to complete our follow-up procedures. The period of review was from May 18, 2017 to June 13, 2017.

A summary of the findings from the original audit report and a summary of the results of our follow-up are provided in the table below. The original findings, management's original responses, and details of the results of this follow-up are contained in the **ORIGINAL AUDIT RESULTS AND FOLLOW-UP DETAILS** section of this report.

Finding	Summary of Original Finding	Follow-Up Results
Finding #1 High Priority	**Journal Entry Audit Trail Not Available**	**A Journal Entry logging feature will be available when the upgrade to PeopleSoft is implemented. The target date for the upgrade is the Summer or Fall of 2018.**
Finding #2 High Priority	**Excessive Number of Employees with Journal Entry Capabilities**	**As of the beginning of project fieldwork, Accounting had not reviewed the list of PeopleSoft users having the ability to create journal entries for the purpose of communicating to DES those users whose access should be removed. The Director of Accounting stated she plans to perform this task shortly after the fiscal year-end of June 30, 2017.**

Finding #3 Moderate Priority	**Locked User Accounts**	**Security roles assigned to terminated employees are being removed by DES. DES can also prepare a report for hiring managers that contains baseline security roles that can be assigned to new employees that replace terminated employees, but the existence of this report has not been formally communicated to hiring managers.**
Risk Observation	**Communication Regarding Changes in Employment Status Recommended**	**As a result of our inquiry, on June 1, 2017 the Office of the CAO issued an email to Commissioners and Directors requiring them to inform DES of any changes in employee status so that PeopleSoft access can be updated in a timely manner. The risk observation is therefore resolved.**

ORIGINAL AUDIT RESULTS AND FOLLOW-UP DETAILS

Original Finding #1: Journal Entry Audit Trail Not Available
Priority Rating: High

Condition:
During a review of the PeopleSoft journal entry controls, we determined that there is no option available to view any edits of journal entries (typically referred to as "journaling"). Therefore, it is not possible to determine if the journal entry being viewed is the original or to what extent it may have been edited. This includes not being certain of the journal entry originator, or of the date and time the journal entry was created.

Effect:
The absence of a journaling feature makes it impossible to monitor changes to journal entries. Without such monitoring, unauthorized changes to original entries may go undetected.

Recommendation:
Accounting should work with Enterprise Solutions to determine if a journaling feature can be implemented in the PeopleSoft financials module.

Director of Accounting Response:
Per DES, functionality in the upgraded version of PeopleSoft will include the ability to log all actions (i.e. create, edit, post, and unpost) related to journal entries. The system will document the action taken, the user that took the action, and the date/time the action was taken.

Commissioner of Finance & Administration Response:
I concur with the Director of Accounting's response

Follow-Up Detail Results:
We were informed that the upgrade to PeopleSoft that will include the ability to log all journal entry actions (create, edit, post, unpost, etc.) has not yet been implemented. This upgrade will probably be completed in the Summer or Fall of 2018.

Director of Enterprise Solutions Response:
I concur.

Chief Information Officer Response:
I concur.

Original Finding #2: Excessive Number of Employees with Journal Entry Capabilities
Priority Rating: High

Condition:
During a review of the PeopleSoft journal entry controls in cooperation with Division of Enterprise Solutions personnel, we determined that 199 employees may have the capability to create journal entries. It is questionable whether there is a valid business reason for so many employees to have this capability. While only the Director of Accounting and four Senior Accountants have the ability to actually post journal entries to the General Ledger, control over the process is increased when users with the ability to create journal entries is limited to those individuals having a clear business need.

Effect:
An excessive number of employees having the ability to create journal entries increases the risk of inappropriate entries.

Recommendation:
Accounting should reevaluate the list of users having the ability to create journal entries, and request that the Division of Enterprise Solutions remove those users who do not have a valid business need.

Director of Accounting Response:
Beginning in January, and annually thereafter, Accounting will request a report from DES containing users with access in PeopleSoft to create journal entries. Accounting will review the list and communicate with users whose access is questionable for an explanation. The communication will include a deadline for response and indicate removal of access if there is no response within the timeframe given. Accounting will generate a final list of those users whose access should be removed and forward to DES for follow up.

Commissioner of Finance & Administration Response:
I concur with the Director of Accounting's response

Follow-Up Detail Results:
We noted during our project fieldwork that Accounting had not yet implemented the action plan provided in the original audit's response. However, the Director of Accounting informed us that she plans on performing this task shortly after the year-end close date of June 30, 2017 as part of the year-end duties. The Director of Accounting also stated that she plans to perform this review on an annual basis.

Director of Accounting Response:
On July 3, 2017, an email requesting the list of users with access to create journal entries was sent to DES personnel. The list will be reviewed for reasonableness and any questions will be forwarded to the Division Director. If necessary, requests for removal of access will be sent to DES. Moving forward, the annual audit will be completed each January.

Commissioner of Finance & Administration Response:
The Commissioner's office will support Accounting to do a review once a year.

Original Finding #3: Locked User Accounts
Priority Rating: Moderate

Condition:
During our review of all PeopleSoft users with the capability to create and post journal entries, we identified numerous user accounts that were "locked". User accounts are "locked" when someone leaves their employment with the LFUCG. The "unlocking" of user accounts can be performed by IT personnel for reasons such as someone returning to LFUCG employment. These "locked" accounts are never removed from the PeopleSoft User table.

Effect:
If an employee returns to LFUCG in a role different from their original job, their journal entry creation rights could be inappropriately reinstated. A terminated user or existing "locked" user could also be inappropriately "unlocked" by IT personnel, creating the risk of unauthorized journal entry creation.

Recommendation:
Enterprise Solutions should delete PeopleSoft user accounts when their employment ends or when their job duties no longer require them to have PeopleSoft access. This process should occur as soon as Enterprise Solutions is notified that someone has left LFUCG employment, or that an existing employee no longer needs the access rights. In the case of a role that is held by only one individual within LFUCG, or no other employees are currently retained in this role, then it is recommended to save this role's user capabilities into a sample user ID named after the position so that if/when this position is filled in the future, the correct access rights are already defined for the new employee.

Director of Enterprise Solutions Response:
DES recommends that PeopleSoft accounts not be deleted, but security associated with accounts be removed. Maintaining accounts is required for analyzing history of transactional entries. DES supports the recommendation that Divisions review and notify DES for changes in security. DES suggests the creation of a report, detailing security roles for a user when change for the user is required. This report(s) would be available to hiring Divisions and DES to provide a baseline security for new employees in the same position. DES does not support the creation of sample user profiles to be saved and/or applied to future hires. Security for new hires should be evaluated by the hiring Division. Over time, roles and responsibilities within a position change. Best practices dictate that security roles be reviewed, identified and assigned during these transitions.

Chief Information Officer Response:
I concur with the remediation steps outlined by the Director of Enterprise Solutions.

Follow-Up Detail Results:
We determined that security roles assigned to terminated employees are being removed by DES. Also, DES has the capability to prepare a report which details security roles for a user when change for the user is required (e.g., when an employee is terminated). This report provides a baseline of security roles that may be assigned to new employees being hired into the same position, and is available only if requested by a hiring manager prior to the terminated employee's roles being deleted by DES. However, the existence of this report has not been formally communicated to hiring managers. DES should issue an email to all Commissioners and Directors informing them of this report and its availability to their hiring managers so that it can be more effectively utilized.

Director of Enterprise Solutions Response:
I concur.

Chief Information Officer Response:
I concur.

ORIGINAL RISK OBSERVATION

Standards for the professional practice of internal audit stipulate that it is the Office of Internal Audit's responsibility to inform management of areas where risk to the organization or those it serves exist. The following observation identifies a risk associated with Journal Entry Controls but does not represent a violation of statures, policies, or procedures. It is considered to be of sufficient importance to deserve mention in this report to ensure senior management's awareness.

Communication Regarding Changes in Employment Status Recommended

During our review of employee capabilities in PeopleSoft, it came to our attention that the Division of Enterprise Solutions is not consistently notified of changes in employee status such as termination or duty changes. If such changes are not communicated to Enterprise

Solutions in a timely manner, employees may retain PeopleSoft access that no longer aligns with their job duties or when they are no longer employed by the LFUCG.

The Division of Enterprise Solutions has a User Request/Modification for Access to PeopleSoft form on the R: Drive under Forms/Infotech. This form should be completed by the responsible hiring/transferring/terminating manager and sent to Enterprise Solutions whenever these types of events occur so that necessary changes to PeopleSoft access can be made in a timely manner. We recommend that the Chief Administrative Officer send an LFUCG-wide reminder to all Commissioners and Directors of this requirement to ensure consistent application of this important process.

Chief Administrative Officer Response:
I agree and will issue the reminder.

Follow-Up Detail Results:
As a result of our inquiry, on June 1, 2017 the Office of the CAO issued an email informing Commissioners and Directors that they must submit a Modified User Form to DES whenever an employee has a change of status, transfers positions, or is terminated, so that necessary changes can be made to the employee's PeopleSoft access in a timely manner. The risk observation is therefore resolved.