Office of the City Auditor and Clerk

FMS Administration

Executive Summary Report

Audit # 10-07

Performed by:

Annie M. Moore

Annie M. Moore, MBA, CPA, CISA, CFE, CPCU, CIA
Manager, Internal Audit

Heather Riti

Heather Riti, MPA, CIA
Senior Internal Auditor

Reviewed and Approved by:

Pamela M. Nadalini

Pamela M. Nadalini
City Auditor and Clerk

Final Report Issued April 22, 2010

10-07 FMS Administration

AUDIT PURPOSE
This audit was included on the 2010-2012 Audit Schedule to review internal controls related to the City's Financial Management System (FMS), as it is a critical application that the city relies upon for financial accounting, reporting and management decision-making purposes.

AUDIT SCOPE
The time period reviewed during the audit was January 1, 2008 to December 31, 2009.

REPORT CONTENT AND LIMITATION OF USE
This executive summary report is limited in detail. In order to obtain the full background on a particular item, please refer to the detailed audit report or contact Internal Audit prior to drawing conclusions based on the limited information contained in this report. Objective ratings indicate the levels at which the objectives were met; rating definitions are included in the appendix (page 4).
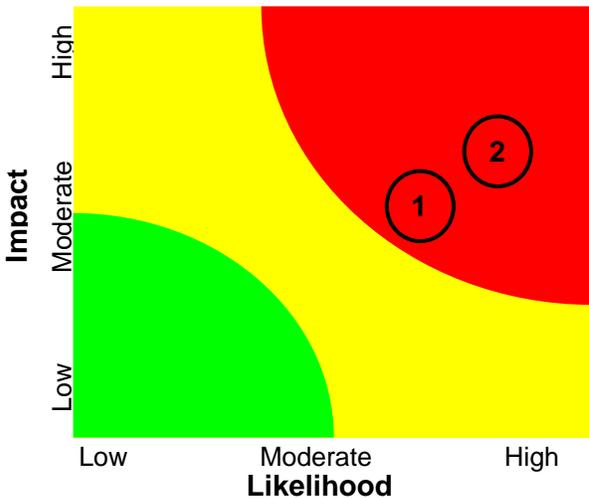
AUDIT CONCLUSION
The results of the audit indicate **OPPORTUNITIES FOR IMPROVEMENT**

This internal audit focused on the following objectives:

Audit Objectives	Objective Ratings		
1. Determine whether controls identified for the business process/functional area were actually in place and functioning as intended; and		X	
2. Determine whether controls were appropriately designed to mitigate or reduce risk.		X	

Significant audit observations (high-priority items) are listed below. For a complete list of audit items, see page 3 of this report.

Risk Exposure Map

Significant Issues	
Observation	Priority
1. The FMS Administrator can currently work directly with the vendor to make changes to the FMS configuration, which is excessive authority.	**High**
2. No formal written policies and procedures for user account administration and monitoring were in place. IT does not currently perform application or user security. FMS Application Administrator has an excessive level of authority as he can modify his own security templates. User activity logging and periodic management reviews of Administrative account activities was not in place.	**High**

10-07 FMS Administration
Observations and Recommendations

Management Action Plans					
Audit Recommendation	**Priority**	**Concur**	**Do not concur**	**Proposed Management Action**	**Action Item Due Date**
1. Formal written system configuration change management policies and procedures should be developed and followed to ensure that a proper change history is maintained and all changes are authorized and justified in writing.	High	X		A Change Management Policy has been developed for the City's Financial Management System (FMS). This policy is intended to document the history of system configuration changes and confirm that they have been properly authorized.	4/9/2010
2. Develop and follow formal written policies and procedures to ensure that user access is properly authorized and kept current to reflect changing duties and is still valid.	High	X		An FMS User Access Policy has been developed to ensure that user access to the software application is properly authorized and updated. This policy will be modified if the Information Security Manager position is funded for the 2010-11 fiscal year.	4/9/2010
3. The two FMS upgrades tested were not installed within 60 days of receipt as required by the contract with Mitchell Humphrey for vendor support coverage. The Financial Administration Department currently receives software upgrades directly from the vendor	Medium	X		The software vendor has been notified to deliver future upgrades directly to the IT Department with a copy of the transmittal letter and performance enhancements delivered to the FMS System Owner. The existing FMS Upgrade Policy has been modified to incorporate the internal audit recommendations. The IT Service Request will include the date that the upgrade was received, the version numbers of the upgrade for both the server and the desktop applications and any documentation that was supplied with the software. The IT Service Request will include a reminder that the upgrade will need to be completed within 60 days of receipt for compliance with our support agreement with the software vendor.	4/9/2010

APPENDIX

Audit Rating System

The audit ratings listed below are based on the auditor's assessment of whether the audit objectives were met.

Red- A red control rating denotes significant business risk or exposure to the City that requires immediate attention and remediation efforts. The controls reviewed do not appear to provide reasonable assurance that the control objectives are being met. The City is being exposed to a high level of business risk and exposure. Management is advised to immediately review the design and effectiveness of existing controls or consider implementing new or additional controls.

Yellow- A yellow control rating denotes opportunities for improvement exist relating to the controls reviewed. If this state of control is not improved, it could lead to a higher than acceptable level of business risk or exposure to the City. The controls reviewed provide some, but not sufficient assurance that control objectives are being met. Management is advised to review the design and effectiveness of existing controls or consider implementing new or additional controls on a priority basis.

Green- A green control rating indicates that the controls reviewed at the time of the audit indicated a satisfactory or acceptable state of control, where risk appears to be minimized and appropriately managed. Controls reviewed appear to provide a high degree of assurance that control objectives are being met. To maintain this rating management is advised to continue to assess the control systems and monitor existing controls for efficiency and effectiveness as business and organizational changes occur.