![City of Sarasota logo]

Office of the City Auditor and Clerk

FMS Administration

Detailed Audit 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

Table of Contents

Background and Introduction

The Financial Administration Department manages and maintains the City's financial management system (FMS), which was developed by external vendor Mitchell Humphrey and Company. The City entered into a license and maintenance support agreement with Mitchell Humphrey in 1998 for a contract term of 30 years.

The City uses FMS to provide an accounting of financial transactions, report on financial data, and maintain capital asset information. All City departments utilize FMS and, at the time of the audit, there were a total of 495 users, 168 of which were active. For fiscal year 2009, nearly 360,000 general ledger transactions were processed through FMS.

Since the initial purchase of FMS, the City has procured various additional modules and reporting tools for the system. The City currently utilizes the following FMS modules: General Ledger, Accounts Payable, Fixed Assets and Purchasing. The City does not use the Accounts Receivable, Cash Tracking, Inventory or Project Ledger modules that are available from Mitchell Humphrey, and instead uses a variety of external systems and records the information into FMS via journal entry. A different vendor/product is utilized by the City for budgeting purposes.

The Financial Administration Department's Accounting Division (Accounting) worked with Mitchell Humphrey on the initial installation and configuration of the application. Accounting performs the majority of day-to-day Application Administrator and Application Owner duties relating to the FMS application, including user administration; setting up the structure of accounts, funds and tables within the system; executing and monitoring batch entries; reviewing and uploading data from other systems into FMS and creating and executing various routine and special-purpose reports. One employee currently acts as the main FMS Administrator and another employee is the primary subject matter expert relating to reports; various employees serve as back-up Administrators when needed.

The Information Technology Department (IT) functions primarily as the Database and Application Administrator as relates to the infrastructure. IT's main role involves maintaining the test and disaster recovery environments, installing and testing connectivity and software, and performing operating system and database and maintenance.

Vendor support related to the application includes notifying the City of and sending available upgrades and troubleshooting questions or problems submitted by Accounting or IT staff relating to performance issues or functionality.

Employees and management of the Financial Administration Department participated in the annual Risk Assessment process in February 2009, which was facilitated by Internal Audit and identified critical risks and associated internal controls for the department including those related to FMS in place as of January 1, 2009. Auditors noted that the department implemented stronger password controls immediately following the 2009 Risk Assessment process.

The Information Technology Department implemented Single Sign On technology after the audit period. Risks and controls relating to this technology will be evaluated in a subsequent audit.

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.

Audit Objectives

The audit focused on the following objectives:

1. Determine whether controls identified for the business process/functional area were actually in place and functioning as intended; and

2. Determine whether controls were appropriately designed to mitigate or reduce risk.

Audit Standards

The Internal Audit Department will have a peer review within the next three years by the Institute of Internal Auditors (IIA). While the Internal Audit Department strives to follow the guidance included in the IIA's International Professional Practices Framework, the *Standards* do not allow the department to note that the department is in accordance with IIA *Standards* until the peer review indicates such compliance.

Testing Methodology

Internal Audit testing included interviews and discussions with management and staff, a business process walk-through, testing of various transactions and a review of available documentation.

Audit Criteria

Conditions found during audit fieldwork were evaluated against criteria for recommended practices outlined in Control Objectives for Information Technology (COBIT) Version 4.1, which the City has adopted as its IT Governance Model.

Noteworthy Accomplishments

Internal Audit noted that the department had prepared and compiled an extensive procedures manual to guide staff in performing the various FMS tasks.

Audit Conclusions

Observations and recommendations in this report are offered as independent guidance to management for their consideration in strengthening controls. In order to maintain confidentially over information security controls, no mention of specific system settings is made in this report.

A complete list of Internal Audit's observations and recommendations is located on page 6 of this report. For information on priority levels assigned to audit recommendations, please see **(Exhibit A).**

The Financial Administration Department has historically performed duties with respect to the FMS Application that are typically performed by an Information Technology Department. This area was noted by Purvis Gray, the City's external auditor, in the 2008 Management Letter and responded to by the City Manager:

> *External Audit Comment:*
>
> ***2008.2*** *- Information Technology - User Access Controls - In some cases, user access controls to computerized applications, i.e., the billing and financial accounting applications, have been decentralized and are under the control of the user department. Best practices would centralize user access controls in the Information Technology Department. User access profiles can be designed by the user departments, but the initiation, termination and management of access should ideally be centralized. Similar to the preceding observation, monitoring controls over user access to computerized applications are also decentralized. We recommend that the City review their policies and procedures in this area.*
>
> *Management Response:*
>
> *We concur with the findings and recommendation. User access for all major software applications will transition from the user departments to the Information Technology Department (IT). The IT Department will become responsible for assigning, terminating and monitoring access to all software applications at the City. User access profiles will be designed by the departments for their software applications. The IT staff will then be trained on user security access for each software application and will assume the role of controlling and monitoring user access.*

The Financial Administration Department continues performing user administration as well as system configuration duties related to FMS rather than the Information Technology Department.

Internal Audit determined through fieldwork and testing that internal controls identified by the Financial Administration Department as part of the 2009 Risk Assessment process were not always in place and/or functioning as intended and, in some cases, were not appropriately designed to mitigate or reduce risk.

While the department did identify various risks relating to FMS Administration during the 2009 Risk Assessment process, certain risks may have been overlooked. Internal Audit has discussed these risks with the department and encourages them to include these as part of the 2010 Risk Assessment process.

Observations and Recommendations

Issue #	Subject	Observation	Recommendation	Concur	Do not concur	Management Response	Committed Action Item Due Date
1	System Configuration Change Management	The FMS Administrator can currently work directly with the vendor to make changes to the FMS configuration, which is excessive authority.	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.	X		Concur. 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	User Access Administration and Ongoing Monitoring	Formal written policies and procedures for user account administration and monitoring (including the titles/names of parties with key roles in the process) were not in place at the time of the audit. IT does not currently perform application or user security. The FMS Application Administrator currently also acts as the Application Owner, which is a conflicting role that provides an excessive level of authority as he can modify his own security templates. A compensating control in the form of user activity logging and periodic management reviews of Administrative Account activities was not found to be in place.	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.	X		Concur. 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	Timeliness of Application Upgrade Installations	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.	Ensure that upgrades are sent directly to IT with notification to the Financial Administration Department. To fulfill the City's contractual responsibilities and to maintain a current version of FMS, test and install upgrades within 60 days of receipt. Ensure that the reasons for not installing any upgrades are documented in the help desk ticket. Retaining a formal record of this FMS version change history may assist in solving any future issues that may arise with the system.	X		Concur. 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

Exhibit A-Internal Audit Recommendation Priorities

Internal Audit utilizes the following classification scheme applicable to internal audit recommendations and the appropriate corrective actions:

Priority Level[1]	Description	Implementation Action[3]
High	Fraud or serious violations are being committed (or have the potential to occur), security issues, significant financial or non-financial losses are occurring.[2]	Immediate
Medium	A potential for incurring moderate financial or equivalent non-financial losses exists.[2]	Within 60 days
Routine	Operation or administrative process will be improved.	60 days to 6 months

[1] The City Auditor and Clerk is responsible for assigning internal audit recommendation priority level categories. A recommendation that clearly fits the description for more than one priority level will be assigned the higher level.

[2] For an audit recommendation to be considered related to a significant financial loss, it will usually be necessary for an actual loss of $25,000 or more to be involved, or for a potential loss (including unrealized revenue increases) of $50,000 to be involved. Equivalent non-financial losses would include, but not be limited to, omission or commission of acts on behalf of the City which would be likely to expose the City to adverse criticism in the eyes of its citizens.

[3] The implementation time frame indicated for each priority level is intended as a guideline for establishing target dates. Determining proposed action dates is the responsibility of the Charter Official(s) over the area(s) or function(s) audited.